防衛装備庁技術シンポジウム2024
特別講演

サイバーフィジカルセキュリティを支える先端技術と課題

2024年11月12日

松本　勉

国立研究開発法人 産業技術総合研究所　フェロー

CPSEC (Cyber Physical Security Research Center) 概要（2024/11）

▶ https://www.cpsec.aist.go.jp/

- 期間: 2018年11月から2025年3月
- ミッション:
  - サイバーフィジカル世界のサプライ/バリューチェーンセキュリティに関する政策を支援
  - サイバーフィジカルセキュリティを測定可能とする研究開発を実施
  - 先端技術の研究開発と知識・人材を蓄積
- 研究センター長: 松本　勉 フェロー
  - 横浜国立大学上席特別教授
  - 基礎から応用に至るセキュリティ研究を1981年から継続して実施
- 構成: 6研究チーム ＋ １連携研究室
- 人数: 100+

- 所在地:
  - 臨海副都心センター（主）
  - 関西センター

伝統的には
秘密計算を含む
高機能暗号技術に
おいて世界的な
強みを有している！

CPSECの研究テーマ群と研究チームの関係

▶ https://www.cpsec.aist.go.jp/

セキュリティ保証スキーム

セキュリティ評価
セキュリティ解析
セキュリティ強化

高機能暗号
ハードウェアセキュリティ
ソフトウェアアナリティクス
ソフトウェア品質保証
CPSECから
デジタルアーキテクチャ研究センターに移動
暗号プラットフォーム
インフラ防護セキュリティ

CPSのセキュリティ保証スキーム確立を目指す

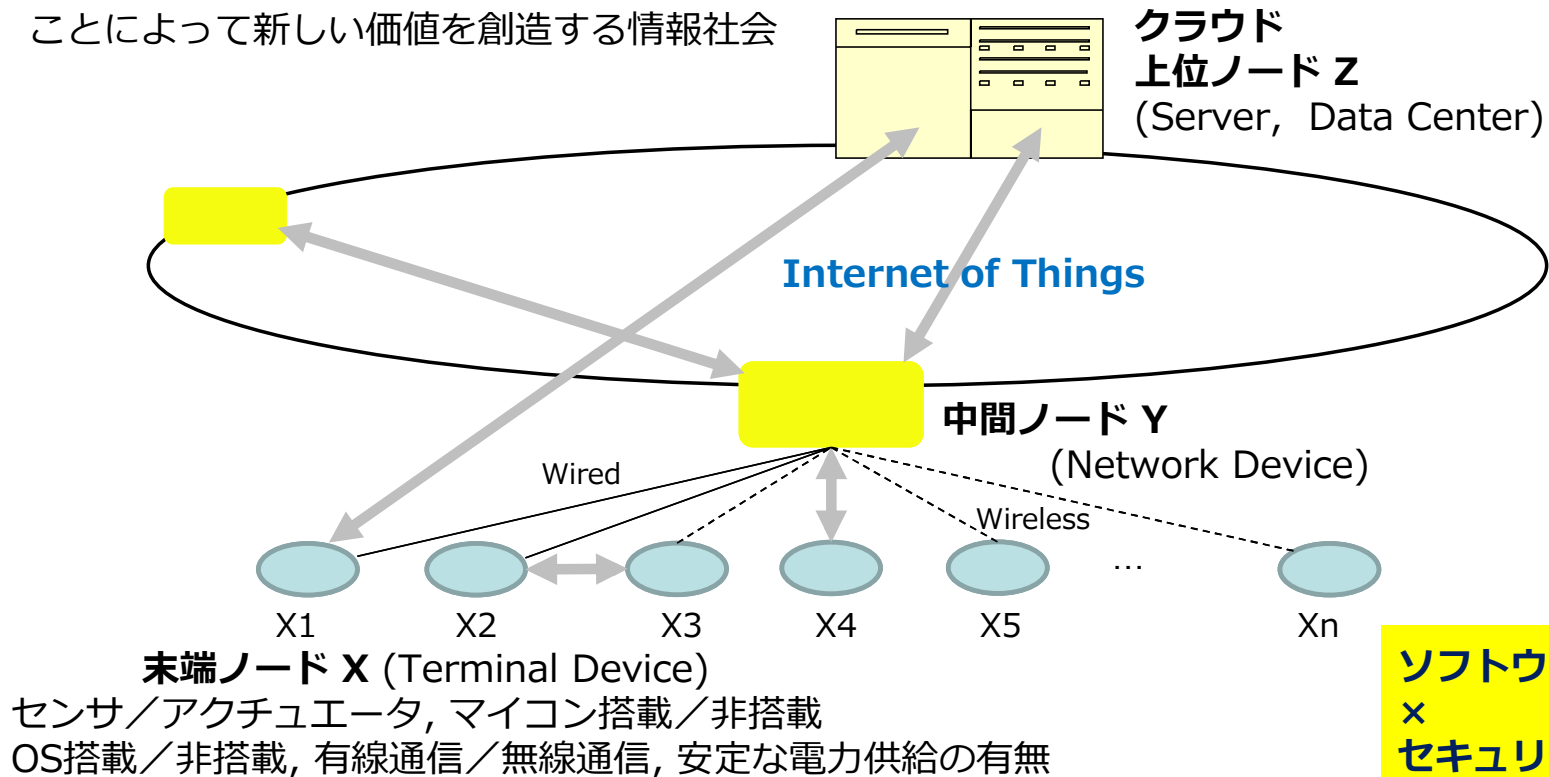
理論　ハード　ソフト　情報システム　CPS

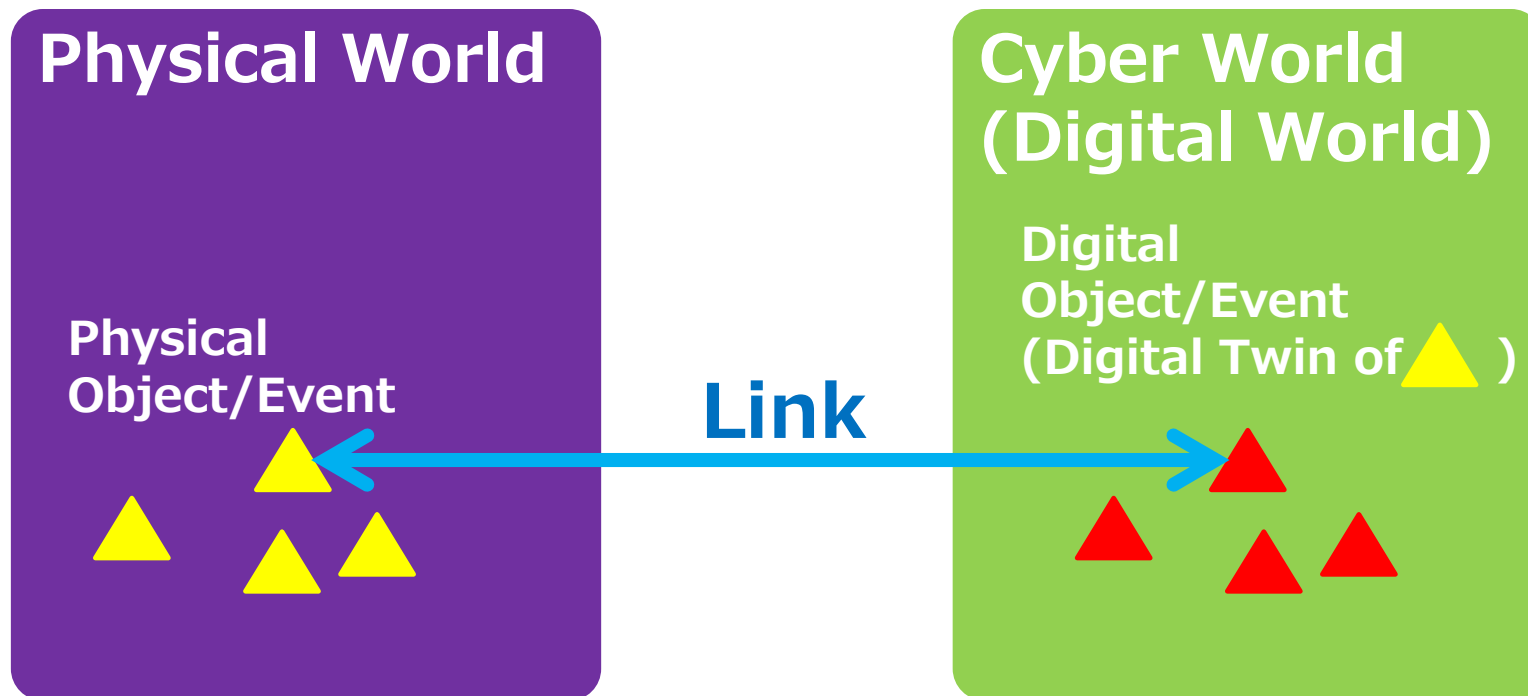
研究分野：暗号技術　ハードウェア　ソフトウェア　セキュリティ認証

サイバーフィジカルセキュリティを支える先端技術と課題　～はじめに～

- サイバーフィジカルシステム、あるいはそれを構成するIoT機器は各種サイバーフィジカル攻撃に対する適切なセキュリティを具備してほしい。
- セキュリティは広範な分野であり、多様な課題がある。
- 例えば暗号技術を用いる場合、あるいは重要情報を扱う場合、関連する方式が論理的にセキュアであるだけでなく、それらに用いられる鍵情報や方式の実装の保護が重要であり、「耐タンパー性」、「耐クローン性」といった性質が求められる。
- この講演では耐タンパー性※を切り口としてお話ししたい。

※ JIS　X 19790において Tamper Resistant = 耐タンパー と記述

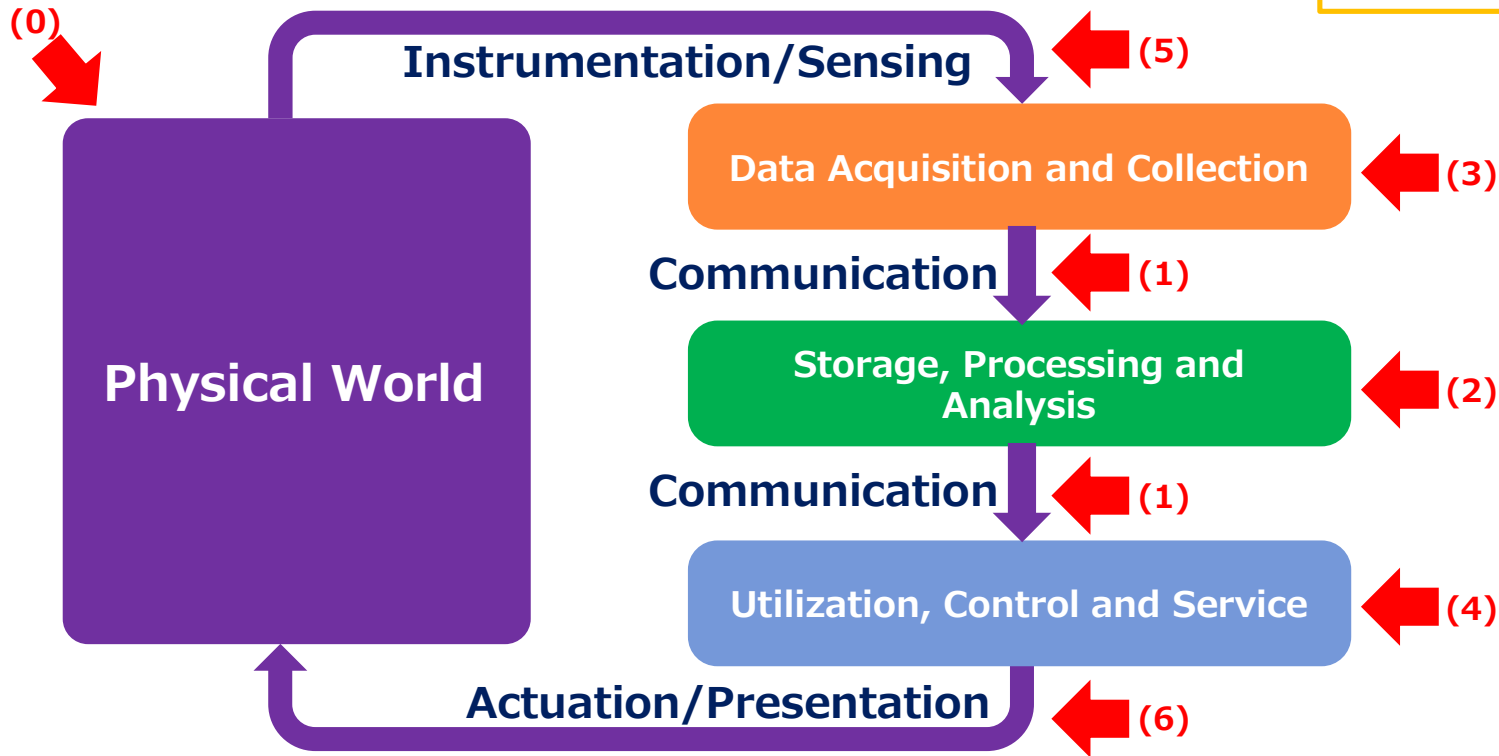
CPS(Cyber Physical System)　IoT(Internet of Things)
～フィジカル世界とサイバー世界を関連付け価値を創造～

フィジカル世界とサイバー（ディジタル）世界
Physical and Cyber (Digital) Worlds

サイバーフィジカルセキュリティの課題

・ID管理／認証
・通信のセキュリティ
・蓄積のセキュリティ
・処理のセキュリティ
・計測のセキュリティ
・制御のセキュリティ
・管理のセキュリティ
・トラストの置き方

- 脅威（攻撃）の分析
- セキュリティの評価
- 対処方針の策定
- セキュリティの強化

> 計算リソース
> エネルギー
> ライフタイム
> 環境変化　※
> 未知の脅威

…
にどう立ち向かうか
> 何を標準化するか
> どうルール化するか

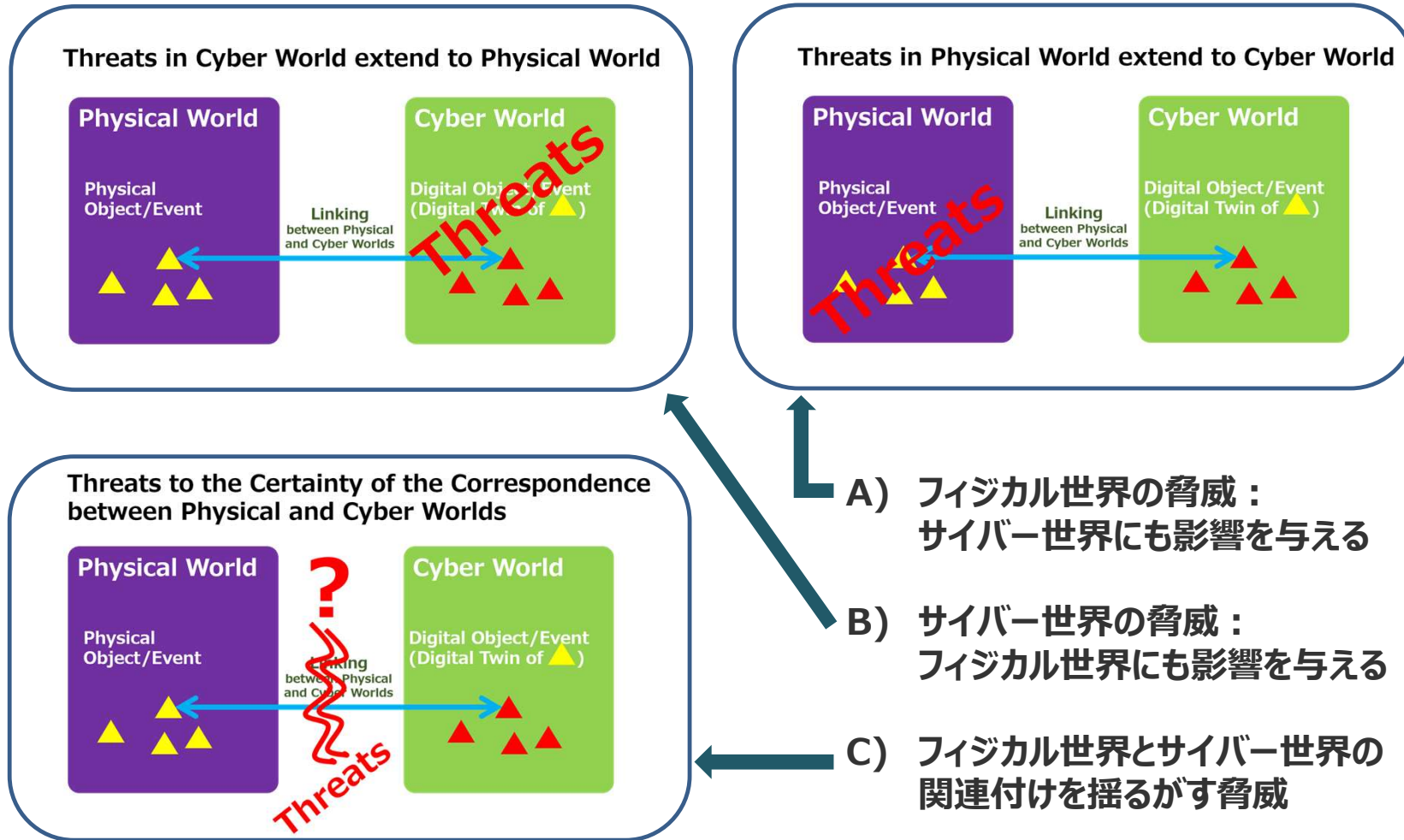
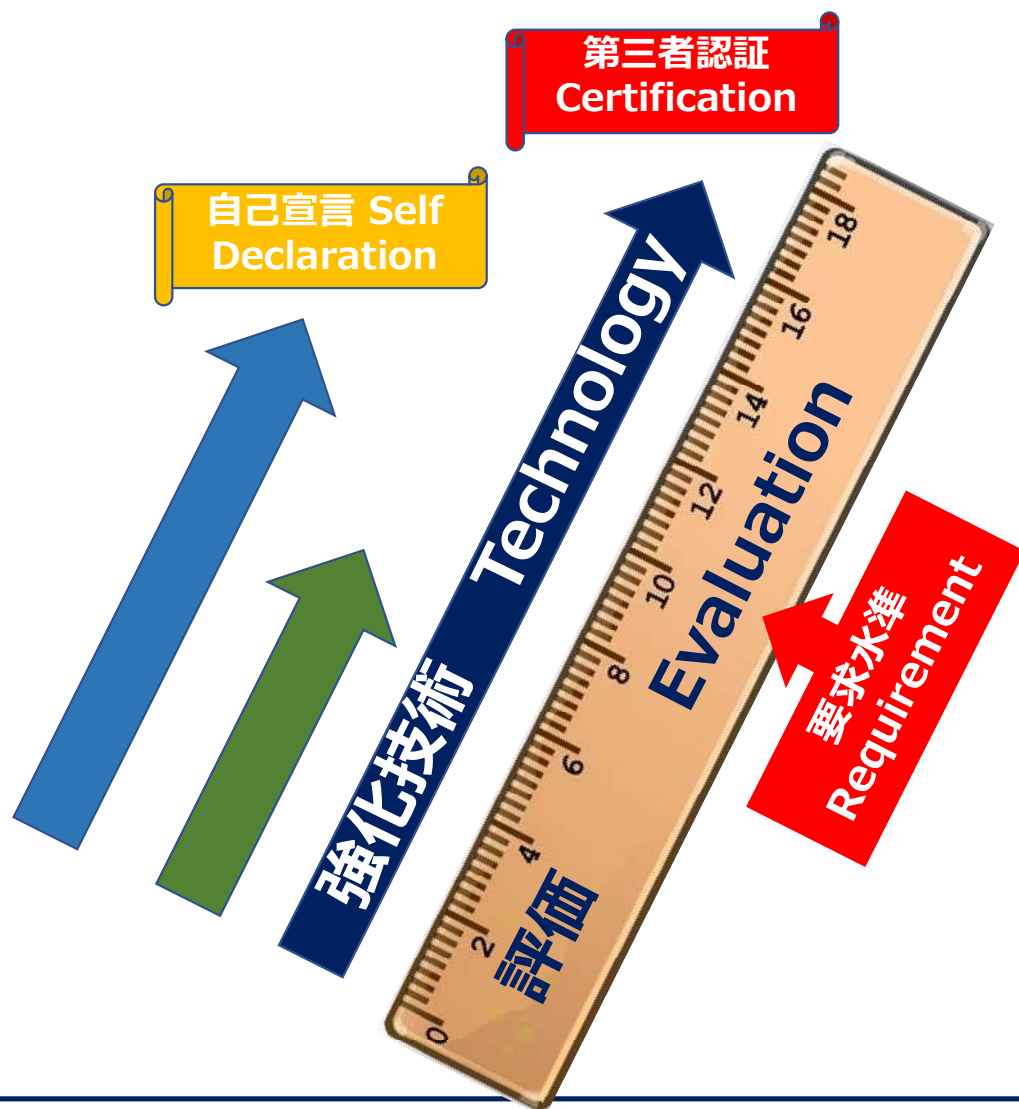
(0)
Physical World
Instrumentation/Sensing (5)
Data Acquisition and Collection (3)
Communication (1)
Storage, Processing and Analysis (2)
Communication (1)
Utilization, Control and Service (4)
Actuation/Presentation (6)

※　技術環境の変化

✓ 通信技術
✓ 半導体技術
✓ クラウド技術
✓ AI技術
✓ 量子計算機
✓ 極限環境
✓ 素粒子
✓ ・・・

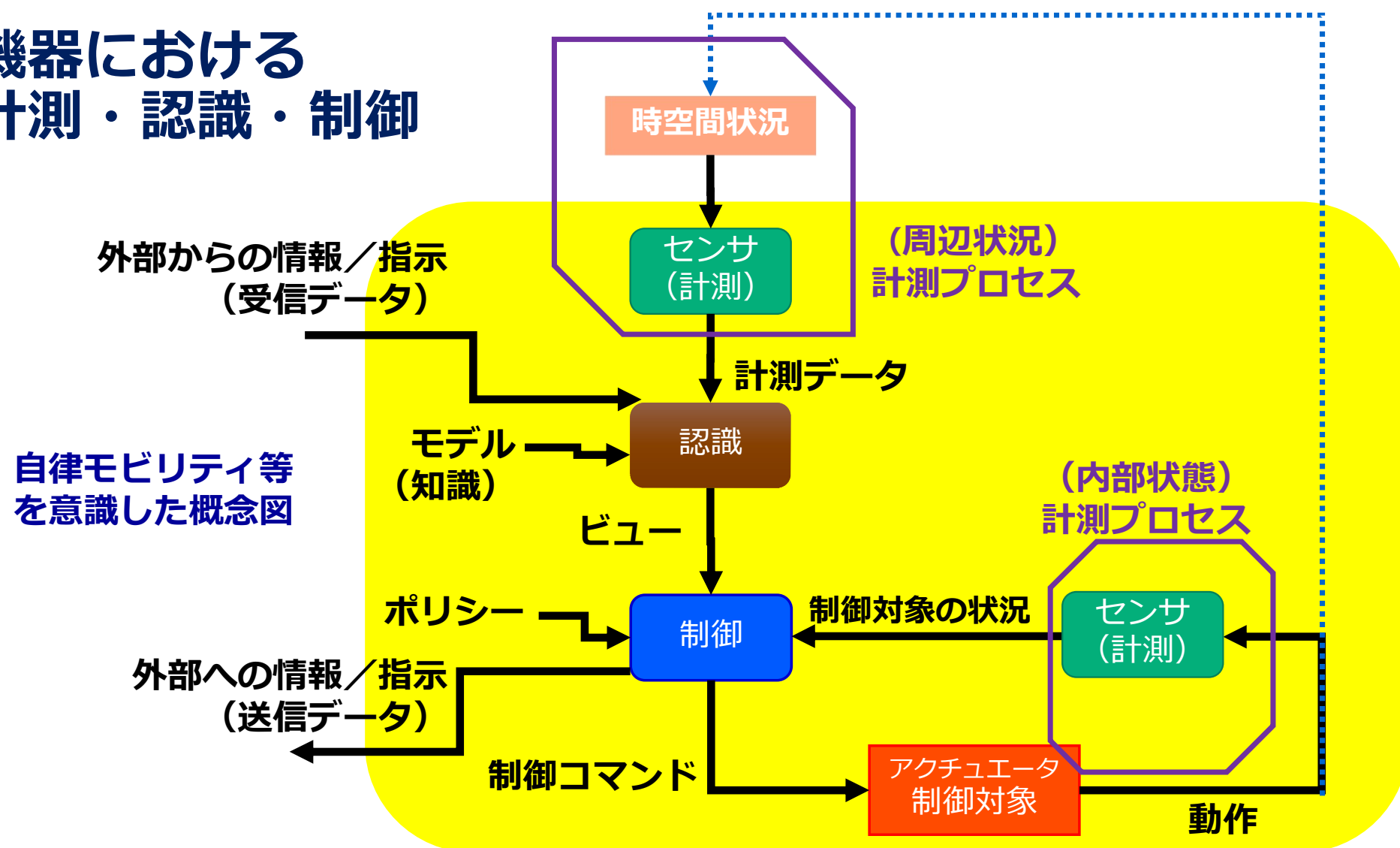
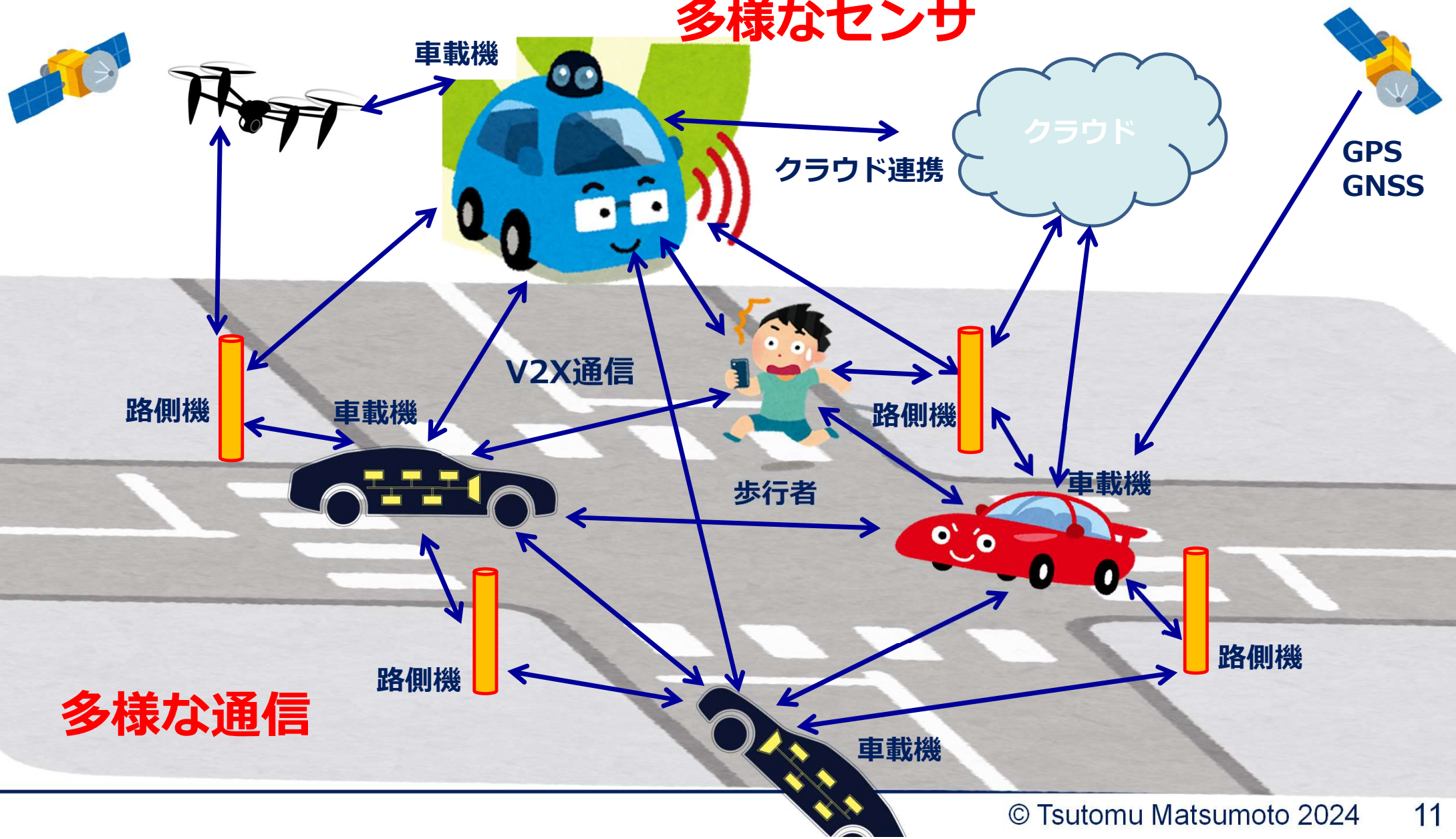
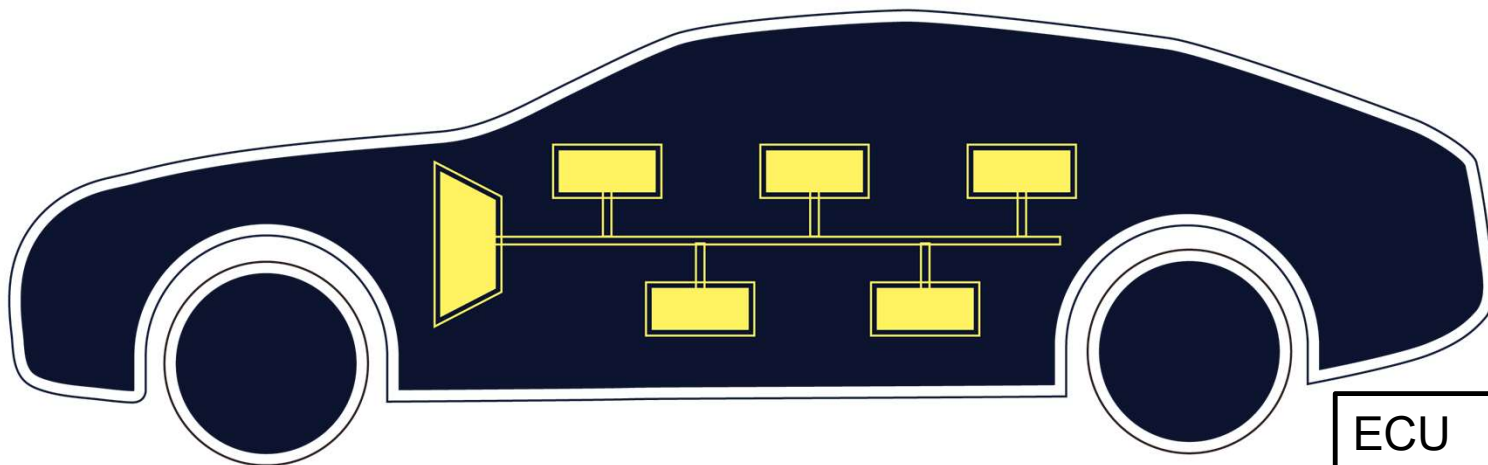
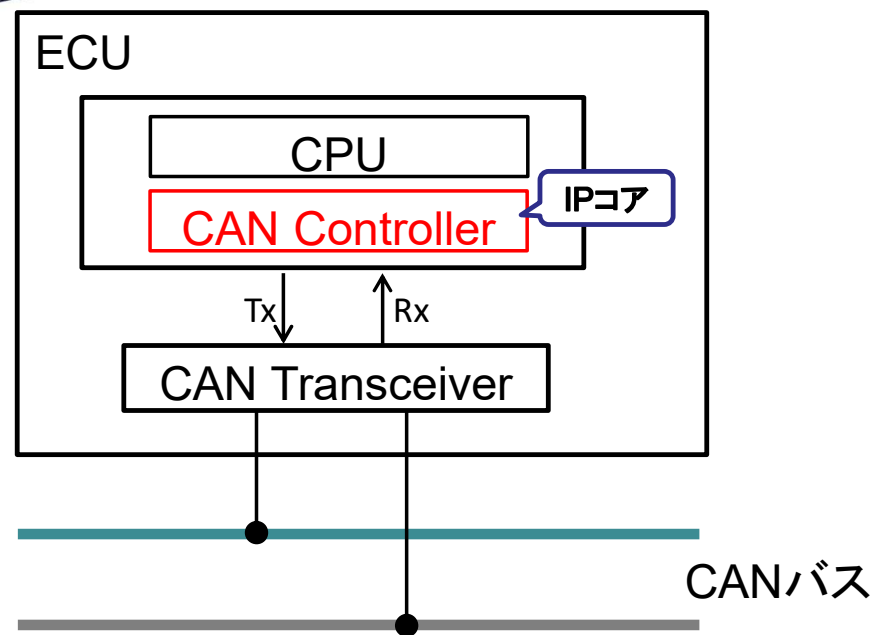
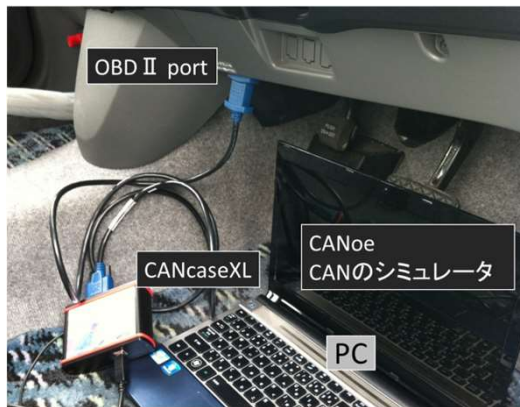
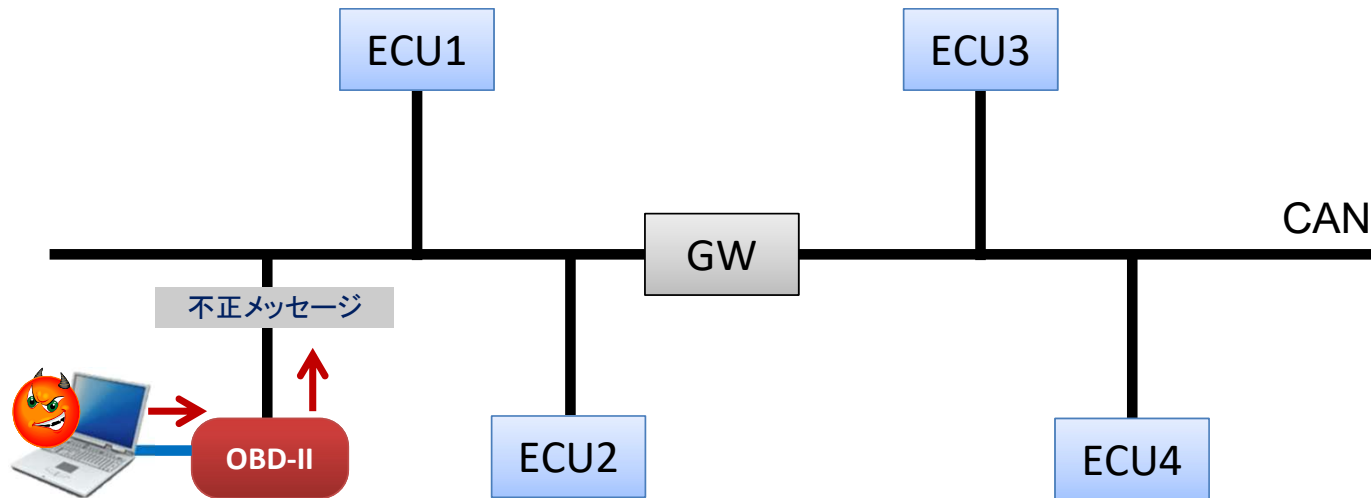
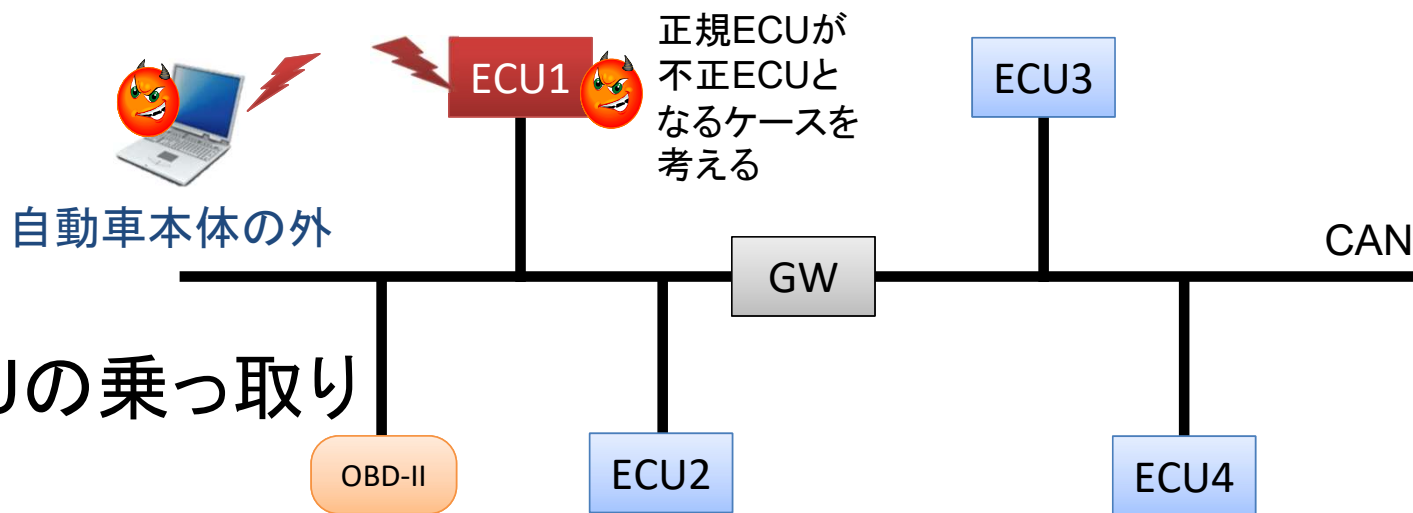
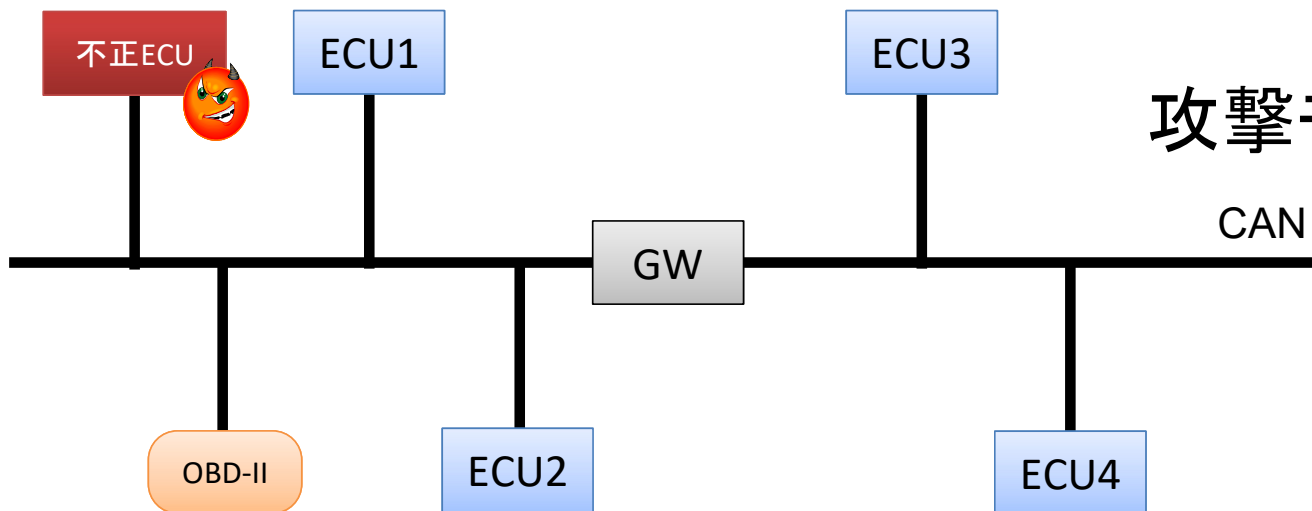
サイバーフィジカルセキュリティに係る脅威は３種類

A）フィジカル世界の脅威：
サイバー世界にも影響を与える

B）サイバー世界の脅威：
フィジカル世界にも影響を与える

C）フィジカル世界とサイバー世界の
関連付けを揺るがす脅威

セキュリティ保証(Security Assurance)

- セキュリティ評価技術
  （Security Evaluation Technologies）
- セキュリティ強化技術
  （Security Enhancement Technologies）
- セキュリティ保証スキーム（制度）
  （Security Assurance Schemes）

機器における
計測・認識・制御
時空間状況
センサ
(計測)
(周辺状況)
計測プロセス
外部からの情報／指示
(受信データ)
計測データ
認識
モデル
(知識)
自律モビリティ等
を意識した概念図
(内部状態)
計測プロセス
ビュー
ポリシー
制御
制御対象の状況
センサ
(計測)
外部への情報／指示
(送信データ)
制御コマンド
アクチュエータ
制御対象
動作

多様なセンサ
車載機
クラウド
クラウド連携
GPS
GNSS
V2X通信
路側機
車載機
路側機
歩行者
車載機
路側機
多様な通信
車載機
路側機

In-Vehicle Network　車載ネットワーク

攻撃モデル1：診断用（OBD-Ⅱ）ポート経由

不正ECU
ECU1
ECU3
攻撃モデル2：不正ECUの接続
CAN
GW
OBD-II
ECU2
ECU4
正規ECUが
不正ECUと
なるケースを
考える
ECU1
ECU3
自動車本体の外
CAN
GW
攻撃モデル3：正規ECUの乗っ取り
OBD-II
ECU2
ECU4

耐タンパー性
Tamper Resistance

0) 暗号の基礎
A) 実装攻撃と耐タンパー性
B) TPM攻撃事例
C) サイドチャネル攻撃研究事例
D) フォールト攻撃研究事例
E) 研究成果のアウトカム

0）暗号の基礎

情報セキュリティ (Information Security)

方針と制御

- **守秘性(Confidentiality)**
  「読む」
- **一貫性あるいは完全性(Integrity)**
  「書く」
- **可用性(Availability)**
  「使う」

暗号(Cryptography)

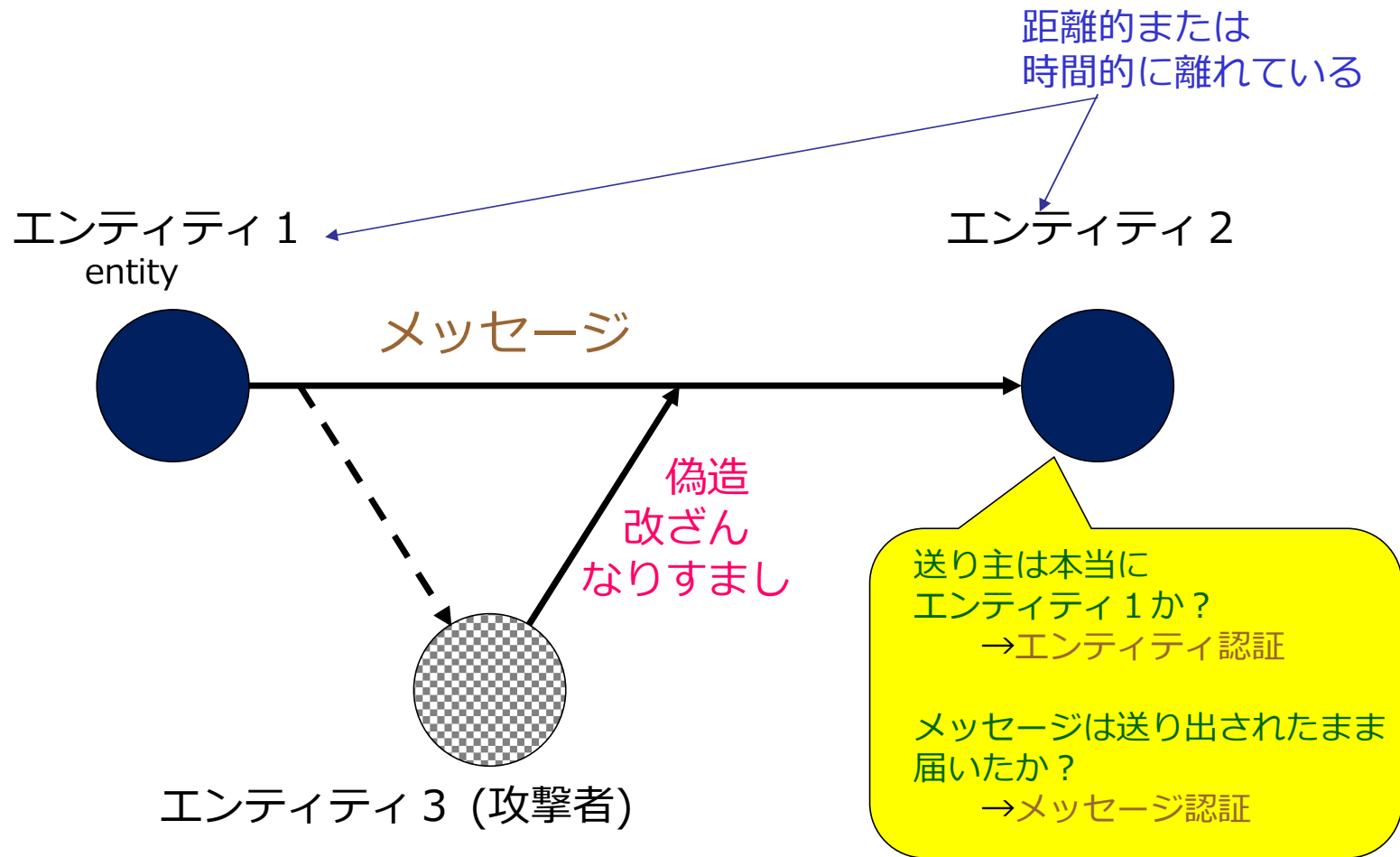
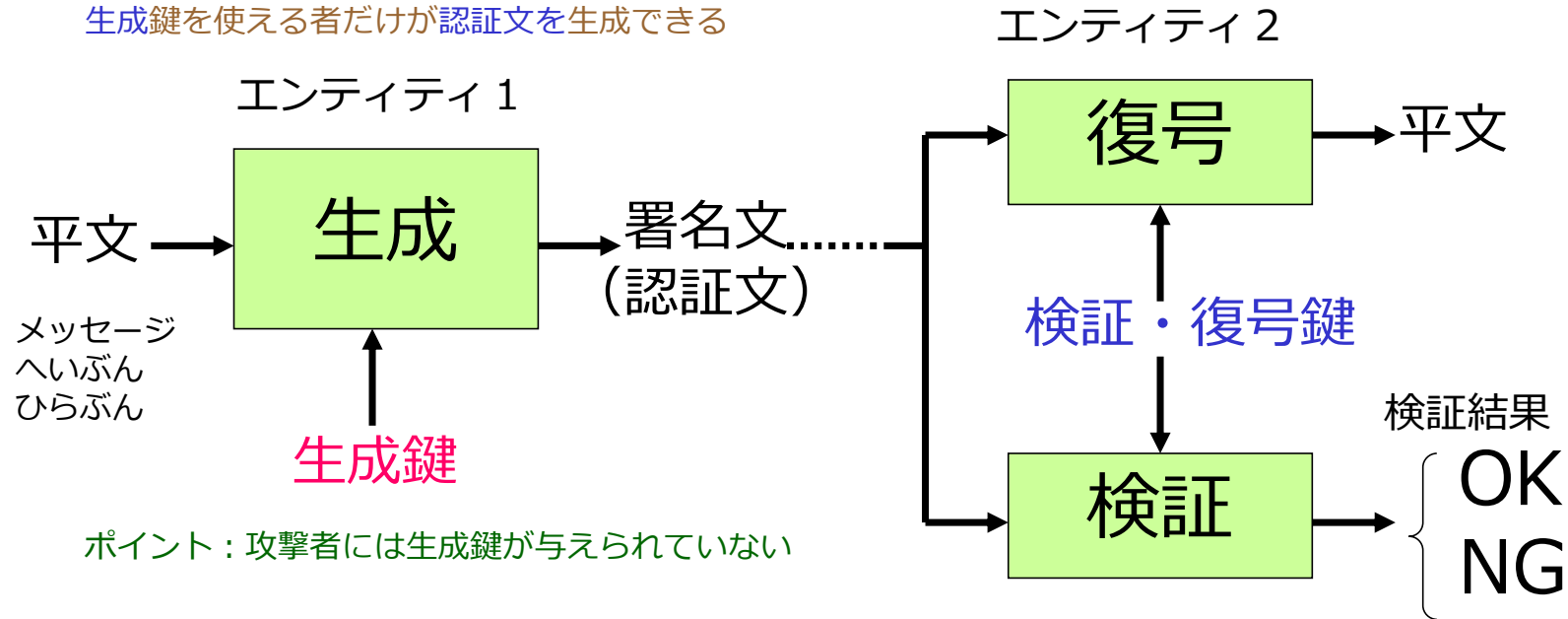
特定の知識（＝鍵）が利用できるか否かにより
特定の操作が簡単に行えるか困難となるかを
制御して

- エンティティの認証
- メッセージの認証
- メッセージの守秘
- メッセージの追跡

などの情報セキュリティを達成しようとする技術の総称

ポイント

- メッセージ処理のアルゴリズム
- 鍵管理のプロトコル
- **実装・評価の方法**

認証(Authentication)の問題

暗号による認証メカニズム

共通鍵認証方式と公開鍵署名方式

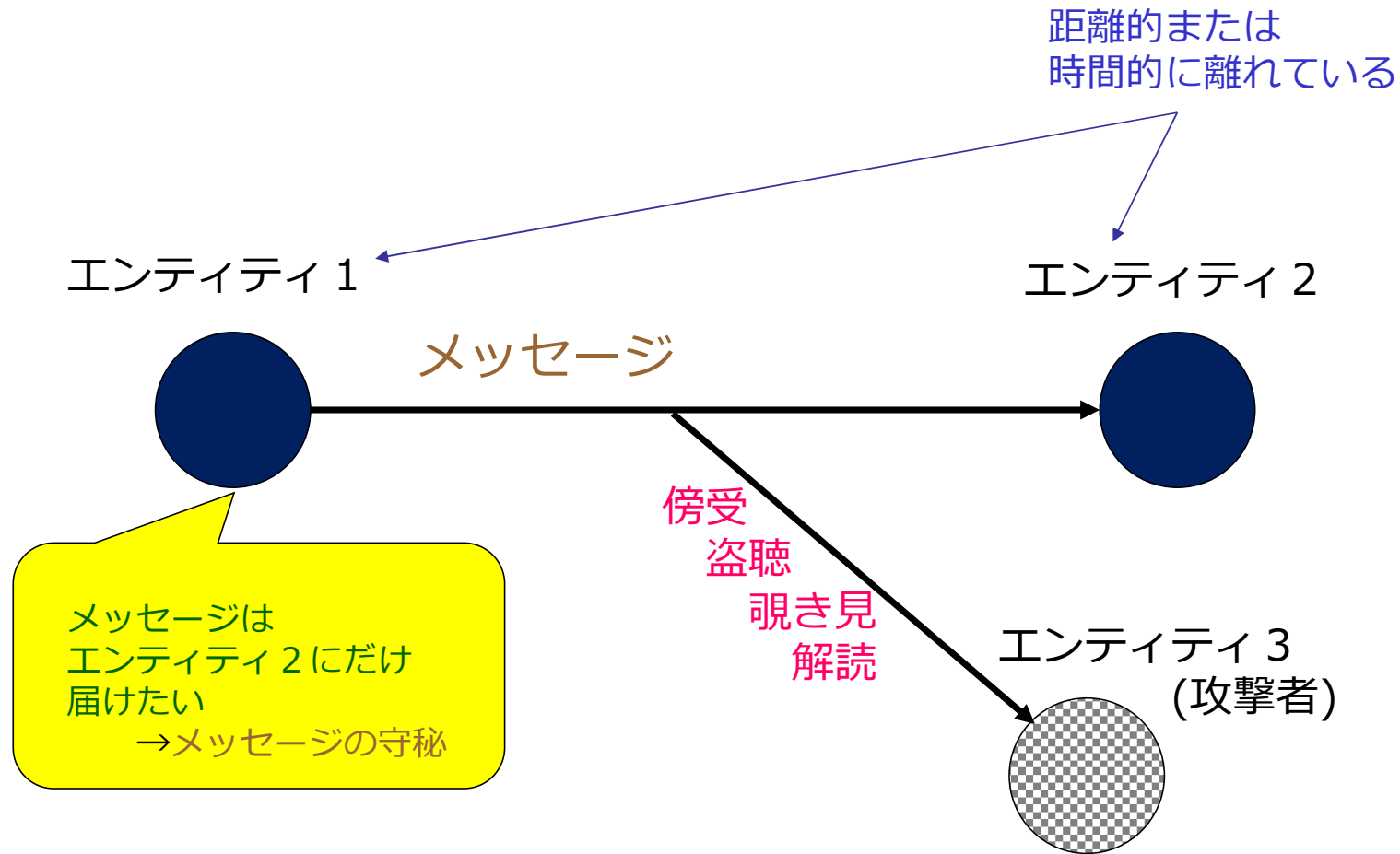
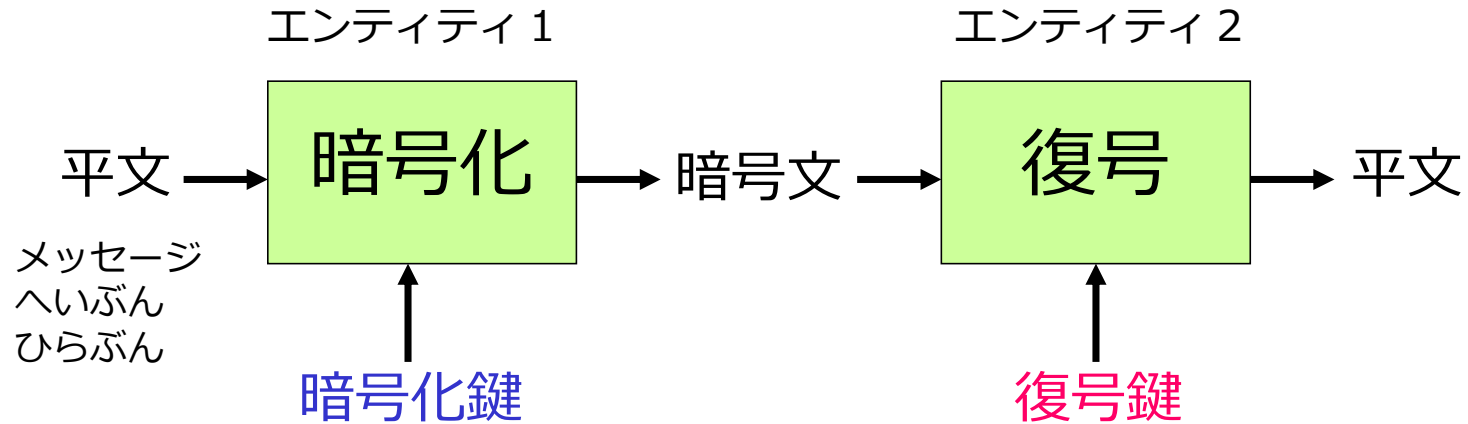
検証・復号鍵から生成鍵を計算することが易しいか困難か

易しい → 共通鍵認証方式

困難（と信じられる）→ 公開鍵署名方式

検証・復号鍵＝公開鍵(Public Key)

生成鍵＝秘密鍵(Private Key)

守秘(Confidentiality)の問題

暗号による守秘メカニズム

共通鍵暗号方式と公開鍵暗号方式

暗号化鍵から復号鍵を計算することが易しいか困難か

易しい → 共通鍵暗号方式

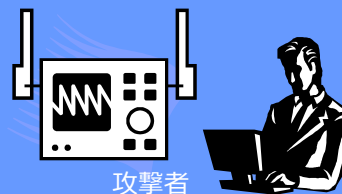
困難（と信じられる）→ 公開鍵暗号方式

暗号化鍵＝公開鍵(Public Key)

復号鍵＝秘密鍵(Private Key)

A) 実装攻撃と耐タンパー性

暗号は多様なシステムに使われている

PCや組込みシステムのセキュリティは
ハードウェアへの情報・物理的攻撃に対する
対策抜きでは語れない.

CANのセキュリティ強化

□暗号技術

1. 車載ネットワークではデータの認証性の達成が焦点であり，共通鍵認証方式であるメッセージ認証コード（**MAC: Message Authentication Code**）の利用が適当.
2. しかし**CAN**ではデータフレームで運ぶことのできるデータ長が高々**64**ビットであり，暗号学的にセキュアとみなされる最低の**MAC**長である**128**ビットすら下回る.
3. このため，**CAN**への**MAC**の適用に関し様々な工夫が提案され，業界標準の手順も整備されつつある.
4. **CAN-FD**において**MAC**適用は本格化すると予想.

□異常検知技術

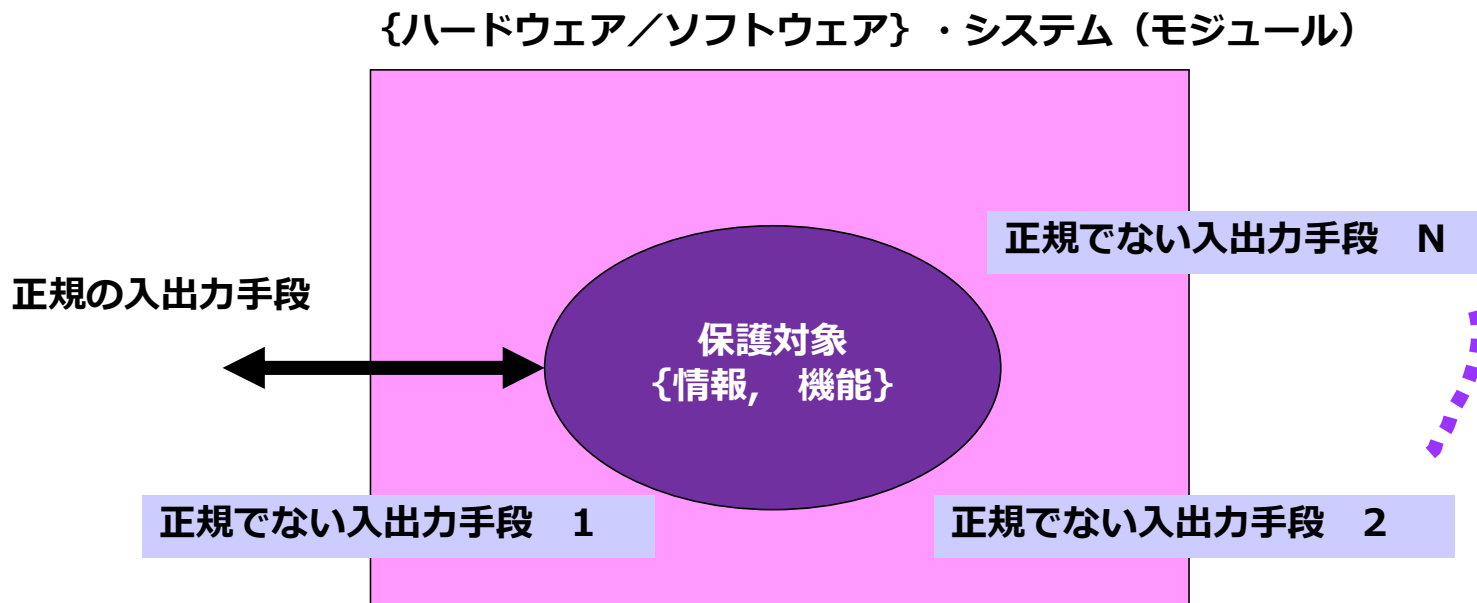
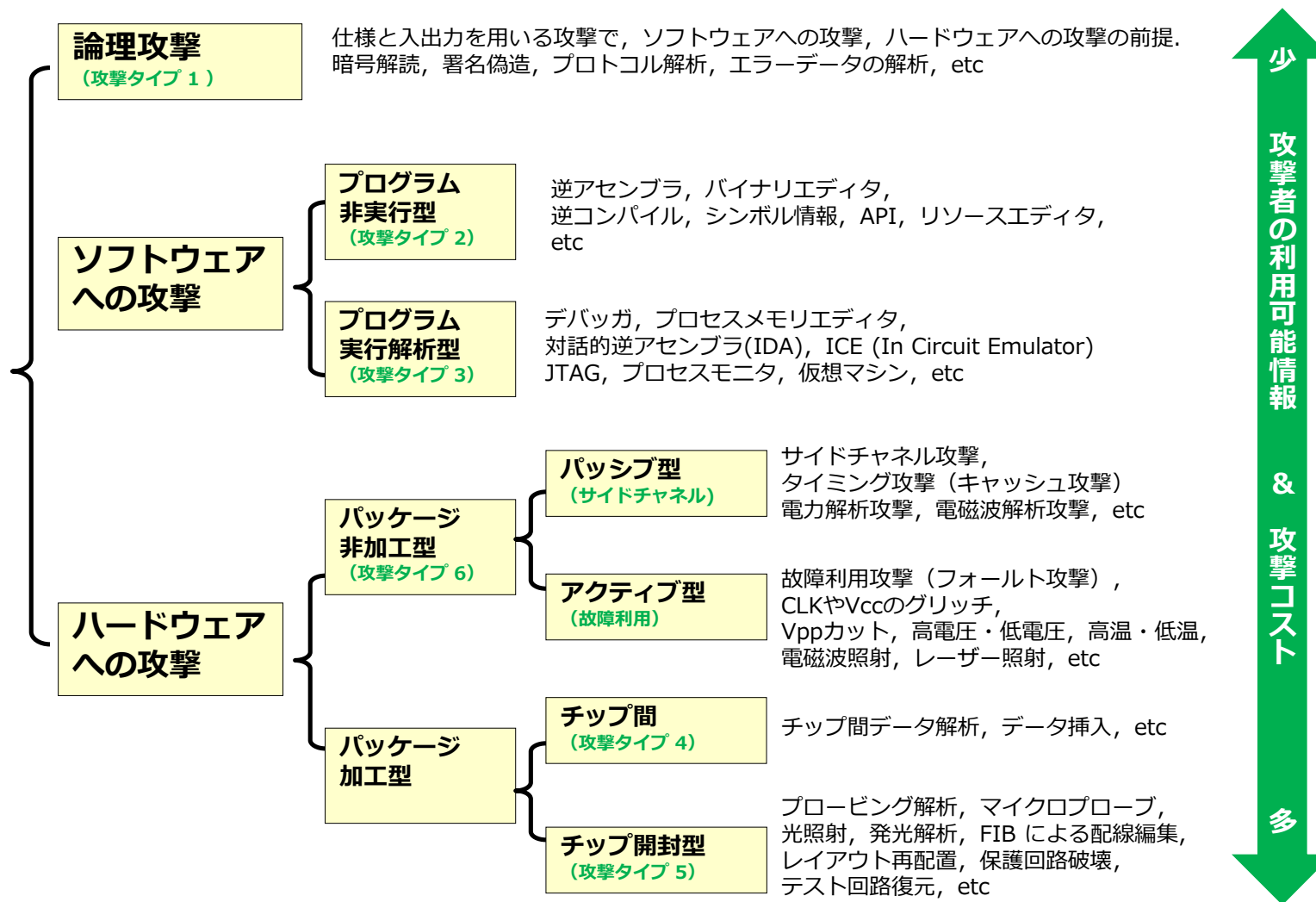
1. **IDS (Intrusion Detection System)** 等を導入することによる車載ネットワークの脆弱性を軽減する保護手法がある.
2. 極めて多様な方式がある模様.

耐タンパー性(Tamper Resistance)

実装攻撃（Implementation Attacks, Tampering, Tamper）に対して
　秘密情報守秘性：システム（モジュール）内の秘密情報を守秘できる性質
　機能改変困難性：システム（モジュール）の機能の改変が困難とできる性質

耐クローン性
Clone
Resistance
は関連するが、
別の性質

＜攻撃をしにくく作る．攻撃の痕跡が残る．攻撃を検出する．攻撃を阻止する．＞

ゼロ化
Zeroization

システム（モジュール）に対する攻撃法の分類

松本 勉, 大石和臣, 高橋芳夫, “実装攻撃に対抗する耐タンパー技術の動向,” 情報処理 Vol. 49, No. 7, pp. 799-809, July 2008.

情報暴露攻撃の例

サイドチャネル情報
消費電力・漏洩電磁波など

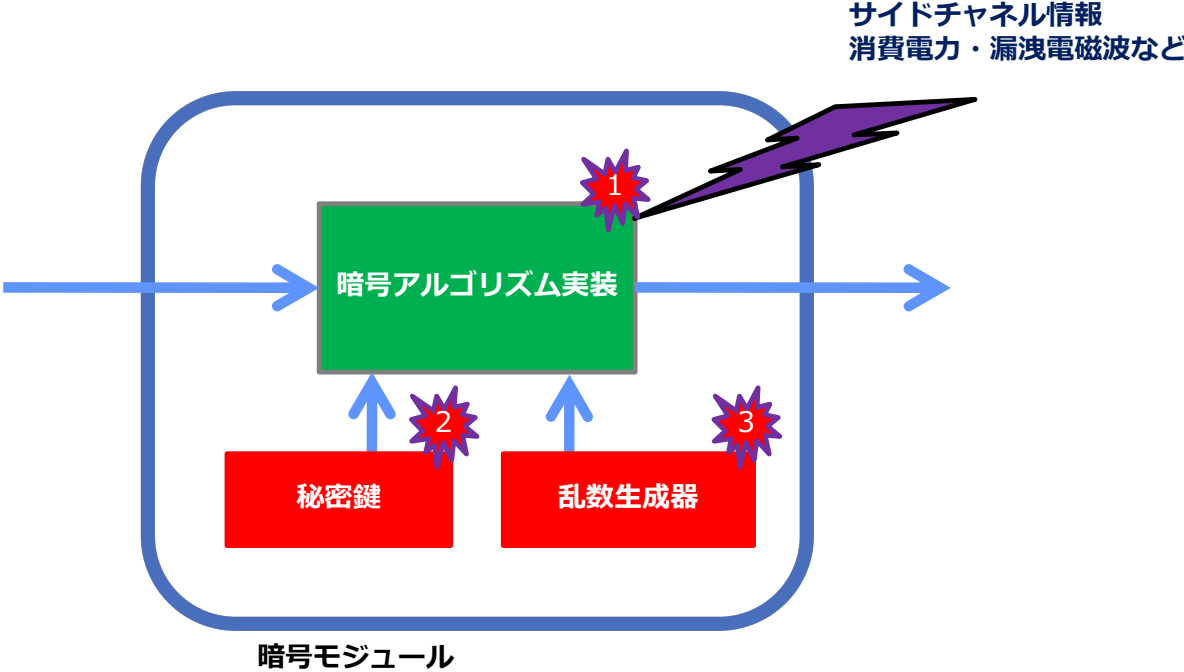
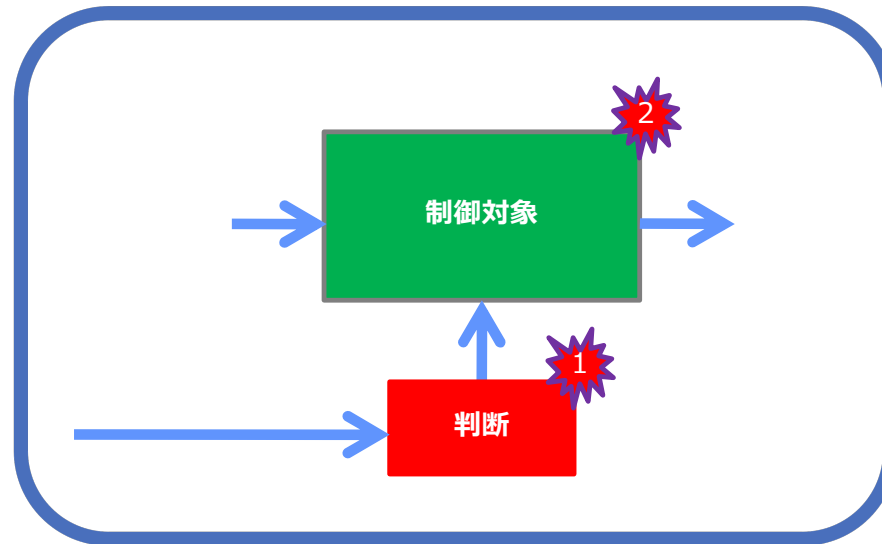
暗号アルゴリズム実装

1

2

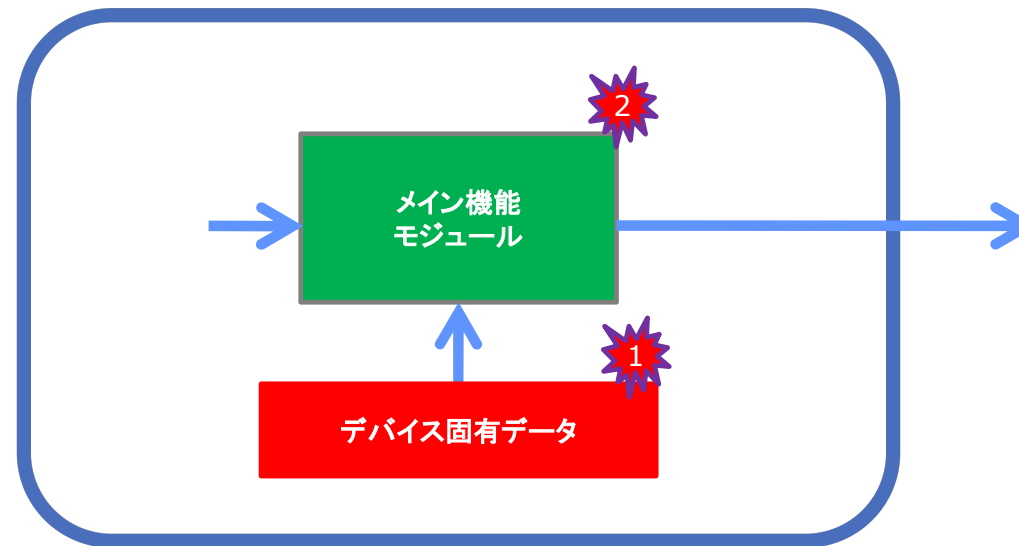
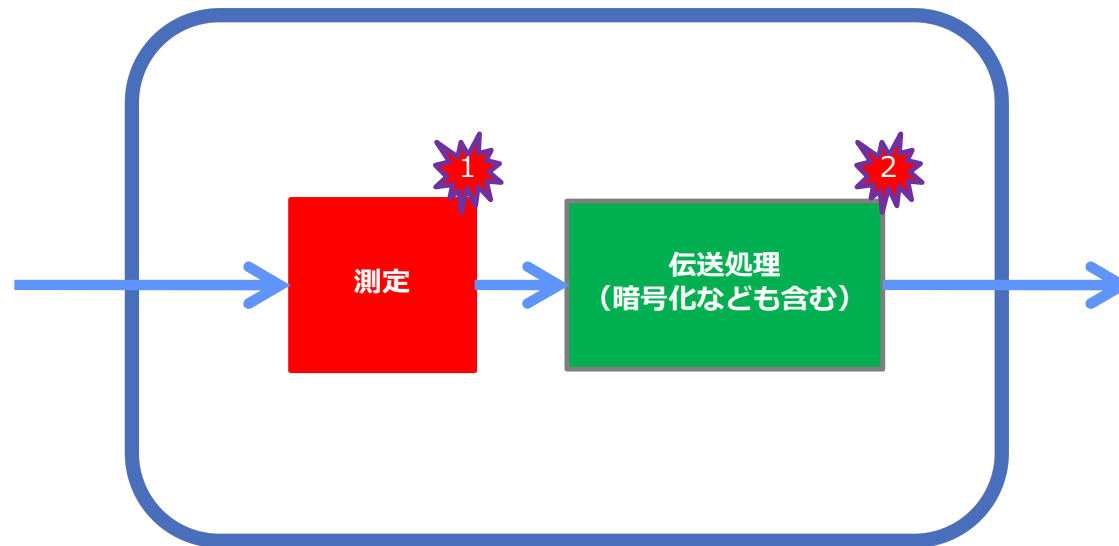
3

秘密鍵

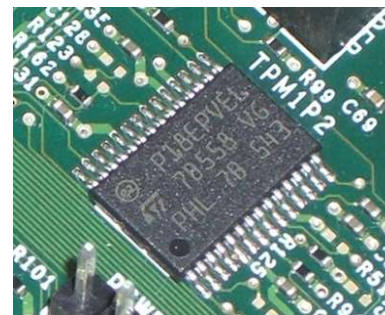
乱数生成器

暗号モジュール

機能改変攻撃の例1

判断に基づき制御を行うシステム
(Tamper Detection, Tamper Response を含む)

機能改変攻撃の例2

機能改変攻撃の例3

B）TPM攻撃事例

ＴＰＭ（暗号モジュールの例）

Trusted Platform Module (TPM) とは，セキュリティチップの一種で，TCG(Trusted Computing Group)が仕様を規格化している．
ノートＰＣへ普及が進み今後は様々な利用が広がる可能性がある．
・物理的にはTSSOP-28ピンのICチップが多く，内部にCPU，不揮発メモリ，公開鍵方式 RSA（法サイズ2048ビット），
ハッシュ関数SHA-1，乱数生成器などを持つ．
・パソコンのマザーボード上では主にLPCバスに接続されていて，ソフトウェアだけでは実現が大変な耐タンパーな
システムの構築のための部品として使われる．

マザーボードに実装されたTPMの例

TPM （TPM利用システム）の攻撃として公表されたもの.

チップ自身に対する攻撃成功例としては，例５が最初のものである．

例1 Replay attack，2005年5月
・プロトコル仕様の不備で，リプレイ攻撃（コマンド実行順序の入替）が可能だった．現在は対処済.

例2 LPCバスのモニタ，2005年9月
・バス上データのモニタ専用ハードを製作し，ブート時のTPMへのアクセス状況を分析して，暗号化鍵を特定.

例3 TPM Reset Attack，2007年6月
・TPMの“PCR”レジスタに対する攻撃．PCRはTrustedBoot等で使用されるレジスタ．TPMのリセット端子をワイヤでショートすると，TPMだけをリセット状態（PCRを０クリヤ）にできる．その後，偽装したいマシンのBIOSやOSのコードをTPMに送ることでPCRを操作できる．現在は対策あり．

例4 Cold Boot Attack，2008年2月
・メモリ上に秘密鍵が残っている間に，冷却/電源オフして，ファイル暗号化の秘密鍵を取得する.

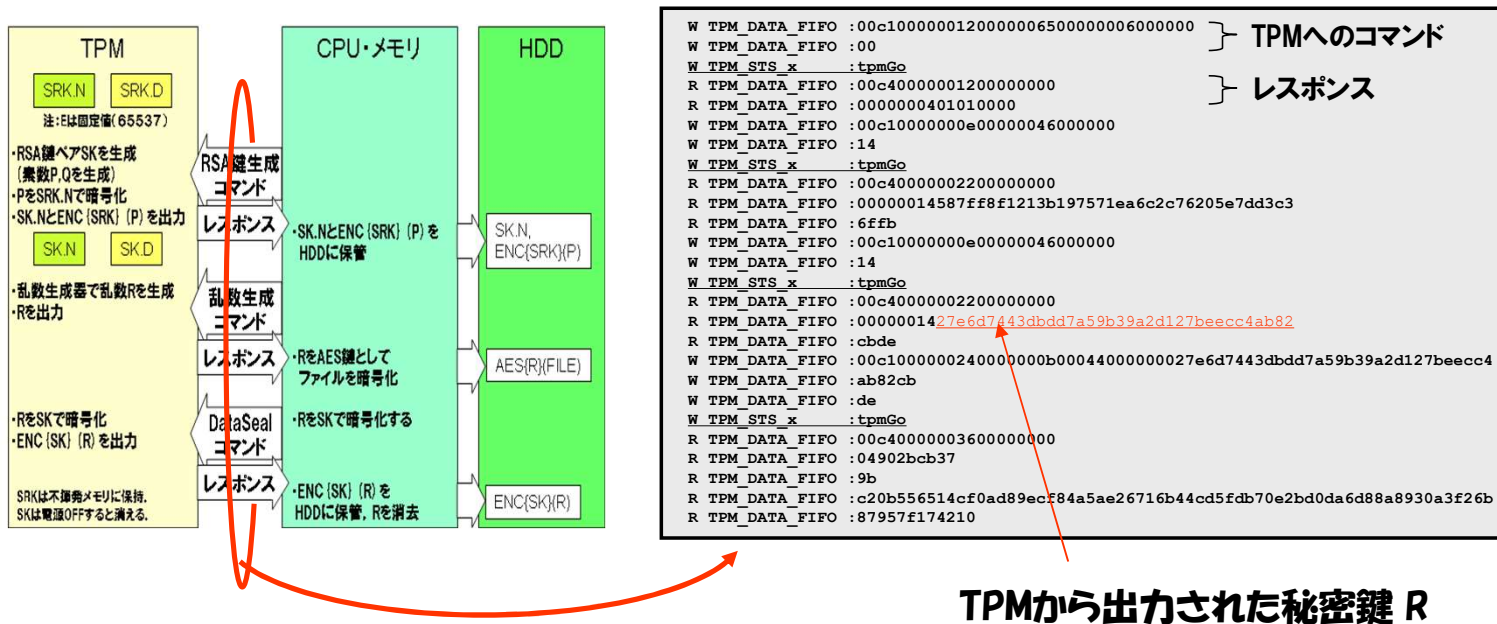
例5 電力解析攻撃，2008年7月
・ある特定のTPMについて，RSA鍵生成中の消費電力パターンから，生成した秘密鍵が解読可能と判明.

例６ パッケージ開封型攻撃，2010年2月
・Infineon社のTPMを物理的に解析して，チップ内のデータバスを特定．バス信号（プログラムコード）を特定.

TPMの攻撃例

例2 LPCバスのモニタ，2005年9月

・バス上データのモニタ専用ハードを製作し，ブート時のTPMへのアクセス状況を分析して，暗号化鍵を特定.

5)モニタ結果．．．．CPUとTPM間のコマンド/レスポンスが全て見える.

・上記の例では，AES秘密鍵Rが平文でLPCバス上を流れるため，秘密鍵が取得可能

TPMの攻撃例

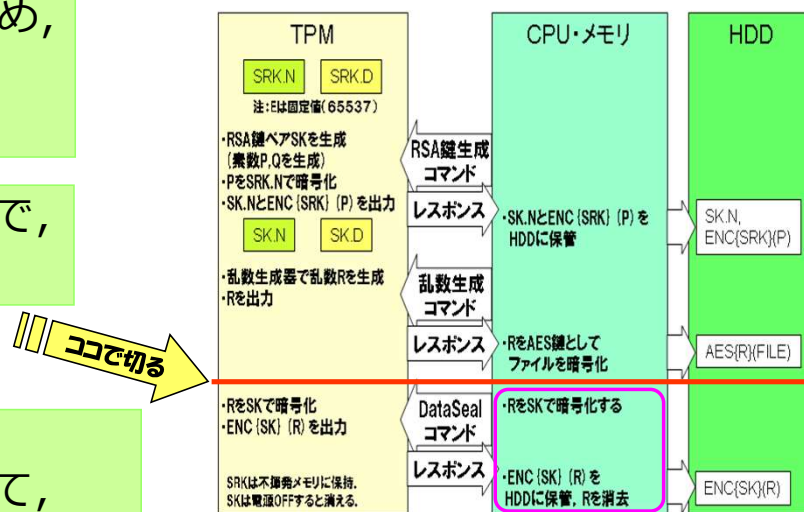
例4 Cold Boot Attack，2008年2月

・メモリ上に秘密鍵が残っている間に，冷却/電源オフして，ファイル暗号化に使用した秘密鍵を取得.

1) DRAMやSRAMなどを冷却すると電源をオフしても，メモリの値（電荷）は，しばらく残存する.
2) この現象を利用し，ファイル暗号化に使用した秘密鍵を取得する.

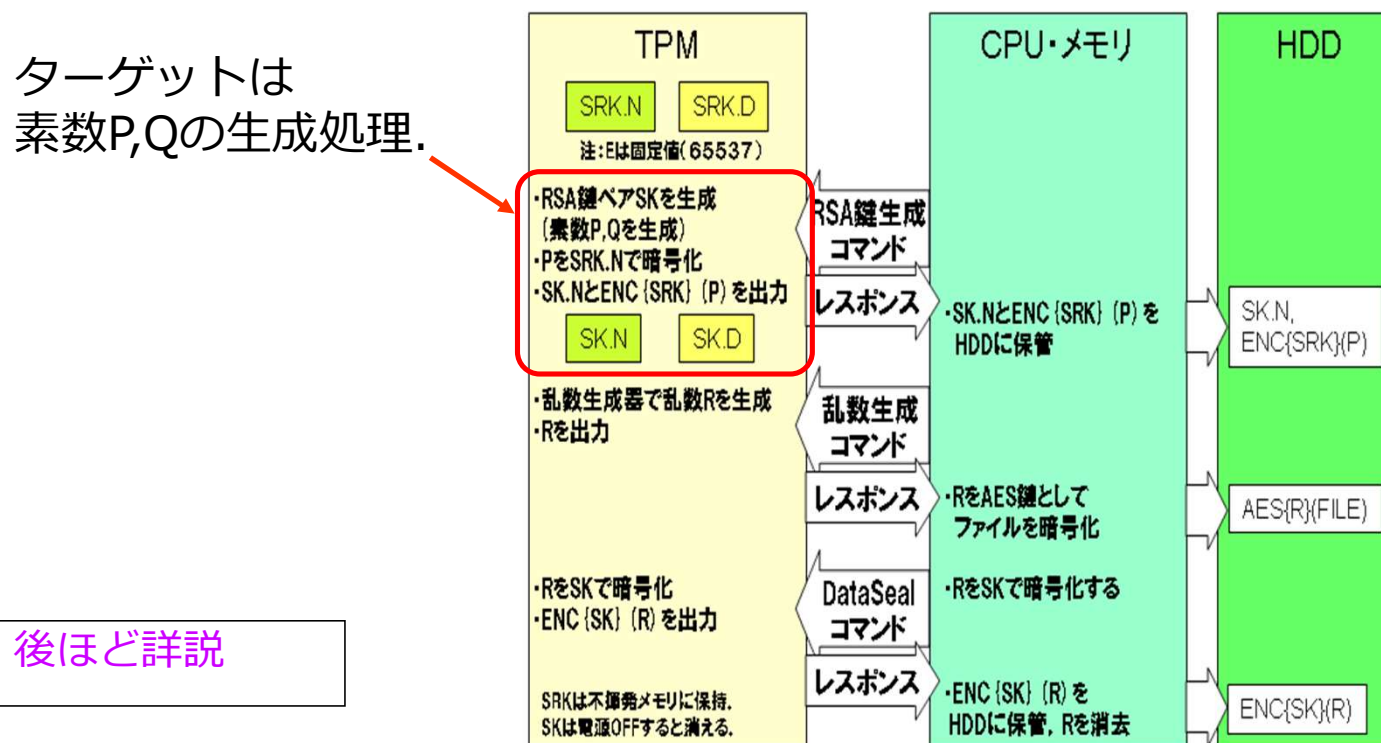
・TPMチップには共通鍵暗号はないため，ファイル暗号化に使用する秘密鍵は必ずメインメモリ上に置かれる.

・秘密鍵がメモリ上にあるタイミングで，メモリを冷却して，電源OFFする.

・残存メモリのサーベイ方法
攻撃者が用意した別のOSでブートして，メモリをダンプする.
あるいは，メモリモジュールを取り外し，別パソコンで読み出す.

TPMの攻撃例

例5 電力解析攻撃，2008年7月

・ある特定のTPMについて，RSA鍵生成中の消費電力パターンから，生成した秘密鍵が解読可能と判明.

1) RSAの秘密鍵はTPM内で生成されて，LPCバス上では暗号化，メモリ上にも置かれない.
2) しかしRSA鍵生成中の消費電力を測定すると，秘密鍵に関する情報を取得できた.

C)サイドチャネル攻撃研究事例

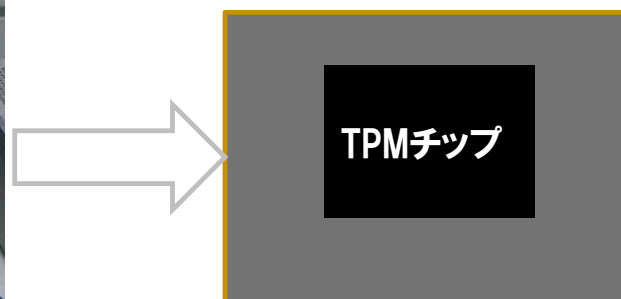
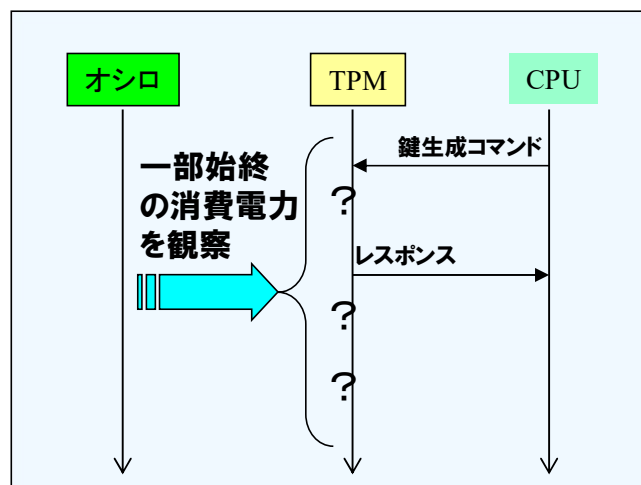
TPMと本体との間の通信データ（RSA鍵生成コマンドに対する応答）

```
TPM_KEY wrappedKey
    typedef struct tdTPM_KEY {
        TPM_STRUCT_VER ver;                       01010000
        TPM_KEY_USAGE keyUsage;                   0011 (=TPM_KEY_STORAGE)
        TPM_KEY_FLAGS keyFlags;                   00000004 (=isVolatile)
        TPM_AUTH_DATA_USAGE authDataUsage;        01
        TPM_KEY_PARMS algorithmParms; typedef struct tdTPM_KEY_PARMS {
                TPM_ALGORITHM_ID algorithmID;     00000001 (=The RSA algorithm)
                TPM_ENC_SCHEME encScheme;         0003 (=TPM_ES_RSAESOAEP_SHA1_MGF1)
                TPM_SIG_SCHEME sigScheme;         0001
                UINT32 parmSize;                  0000000c (=12 byte)
                [size_is(parmSize)] BYTE* parms;
                    typedef struct tdTPM_RSA_KEY_PARMS {
                        UINT32 keyLength;         00000800 (=2048 bit)
                        UINT32 numPrimes;         00000002 (=two prime)
                        UINT32 exponentSize;      00000000 (=0 byte)
                        BYTE[] exponent;          {nul}
                    } TPM_RSA_KEY_PARMS;
            } TPM_KEY_PARMS;
        UINT32 PCRInfoSize;                       00000000
        BYTE* PCRInfo;                            {nul}
        TPM_STORE_PUBKEY pubKey; typedef struct tdTPM_STORE_PUBKEY {
                UINT32 keyLength;                 00000100 (=256byte)
                BYTE[] key;                       b272bda6b2f8924c8fd64a6e8a53c109 6ee115e05c610b3da7fe4faeef2a0cf6
                                                  3ec07ddd40901dec92a1d494533be2db e47c6c69979f6fa2d0f305da678a3a30
                                                  58833047f73a42333935ccf7f138c3f3 2575b39ef0d84867f09316f582ae2c4e
                                                  bf4e6c95963a4b9a96cab0b019e295b8 4aa6aace4a6d4df0c11972aaf1f2d223
                                                  fc2a10a958206eebfb1460babd3113a5 90898e01cc7e6fccccfddb8429db7380
                                                  207435d0412f90203d8193cc0dfe769c a7ae672c8aca164eebc46b1e32d51e9e
                                                  f6e3c3b49ea749a6941de283c992a0ad cb1f1d8cbe7f00842246b8731353ec02
                                                  44bc2df0a60e9b868ab48bd8cd0634e9 9abd5708a3a1e745c12e57fdd1c8a5d1
            } TPM_STORE_PUBKEY;
        UINT32 encDataSize;                       00000100 (=256 byte)
        [size_is(encDataSize)] BYTE* encData;     d0e907fd942a368fbb04bdfc273954fc da2a9133c82a33f7c0b6d5f9e0420fdc
                                                  2f78c5348eca28376460a8b1ea1a1a16 bedfada187426a8726f0b40ab47e3e58
                                                  79f82edb5a288b8c179b8709d1921339 0504e345de7f5fe70e9913235df9daa7
                                                  ef3d4e139563a67fb672d051fcd73168 150bdabfe79f6cf5248b1f4bd32600c0
                                                  5b4dc08ecede3ca78d5fe42f4e66e591 9c029b900b61510fcd908ef286227b47
                                                  6e1956dbbefb92766498f78d4c19c640 7f4893aa47348e70d774d43d9b210827
                                                  fdccd7d4cd712fe4482246a79260005b 9485a8affa880cdcbe7f09cb070ff643
                                                  4595ed2673721bb7c0341714070edf1d 8556b05463468043249fa6d9a4a49353
    } TPM_KEY;
```

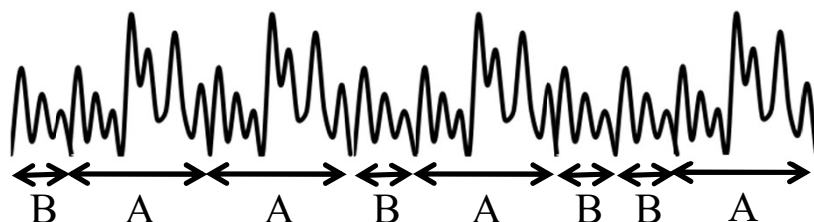
この256バイトが公開鍵（SK.N）

こちらの256バイトは128バイトの秘密鍵（SK.P）を暗号化したもの

TPM内での鍵生成処理の観察

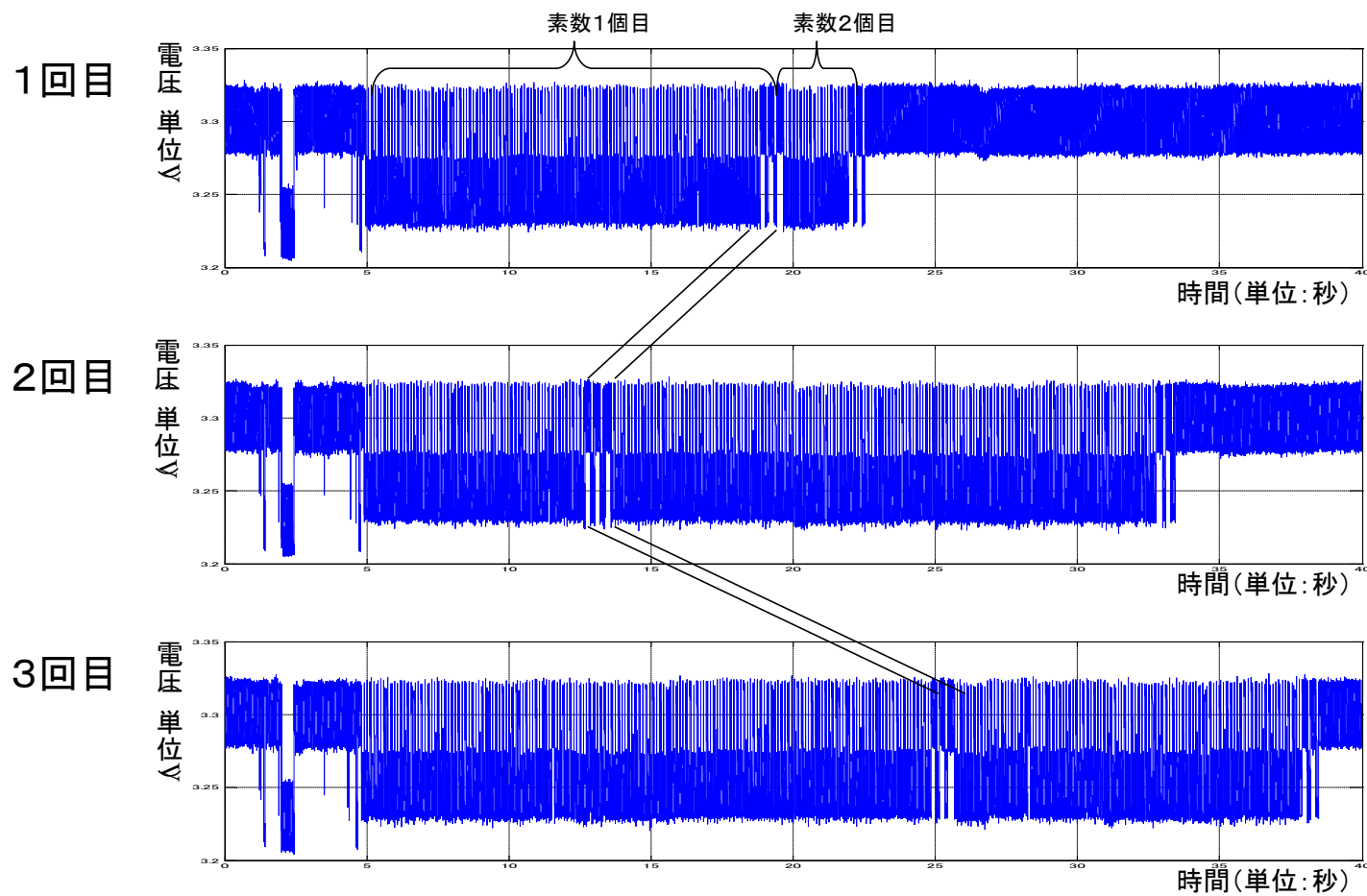
あるTPM（実製品）のRSA鍵生成処理の消費電力をオシロスコープで観察した.

単純電力解析・単純電磁波解析の原理

演算にAとBの2種類があり、それぞれを実行したとき
に観測される消費電力波形または電磁波の波形が

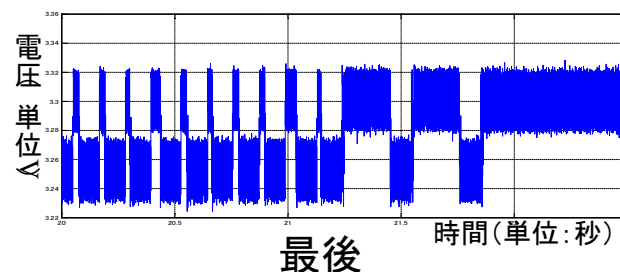
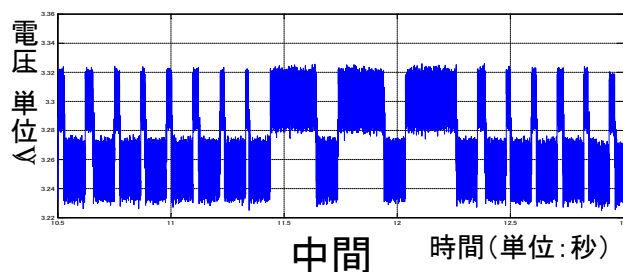
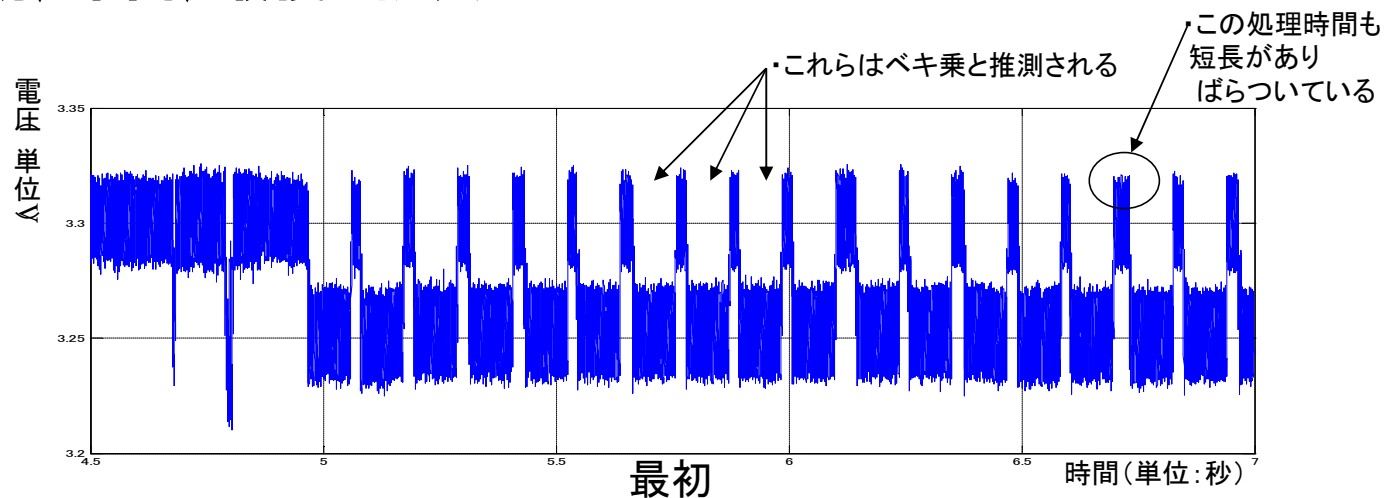
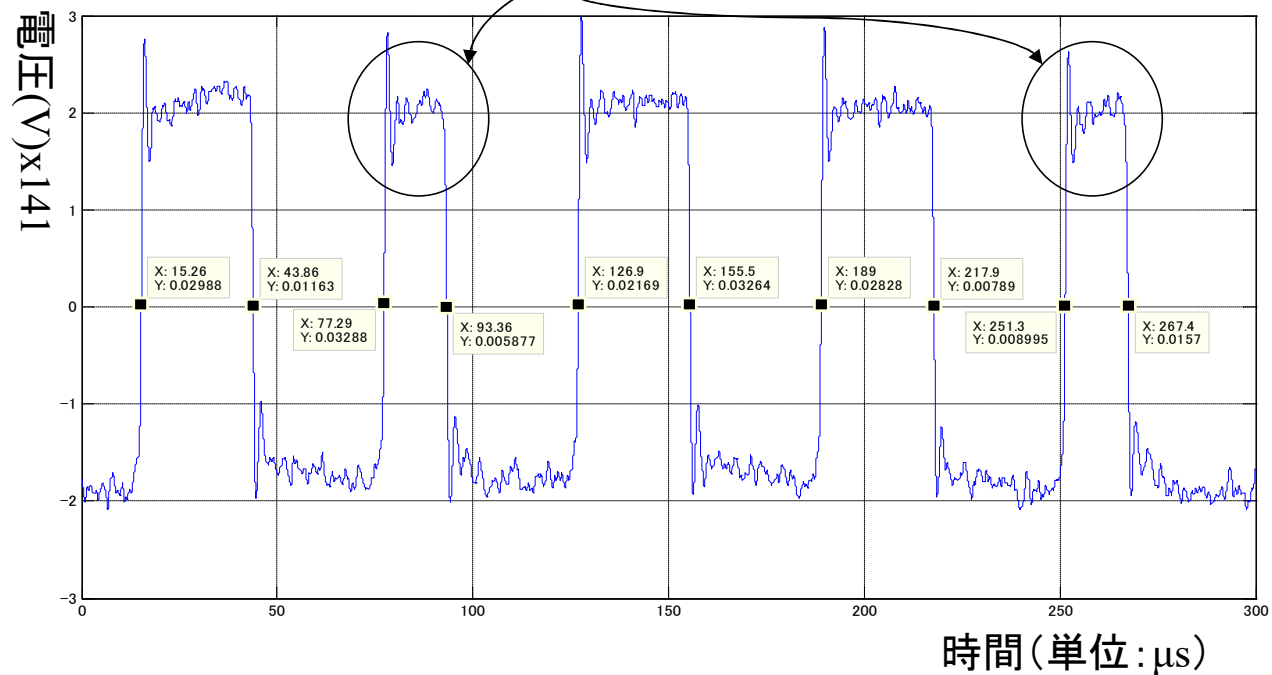
のように異なることが分かっているとする。攻撃者にとっては
未知の鍵Kに基づく計算をICチップが行う際に、波形として

が観測されたなら、波形から演算が

BAABABBA

という順番で実行されたことが分かる。この順番を示す情報が
すなわち鍵Kであるなら、波形から鍵が推定できたといえる。

TPM内での鍵生成処理の観察（1/3）

TPM内での鍵生成処理の観察（2/3）

最初／中間／最後を拡大

次々と素数判定している様子が反映されていると推測した.

TPM内での鍵生成処理の観察（3/3）

TPM内で生成された秘密鍵の解読

RSA鍵生成コマンドのレスポンスから，公開鍵 **N**を取り出した：

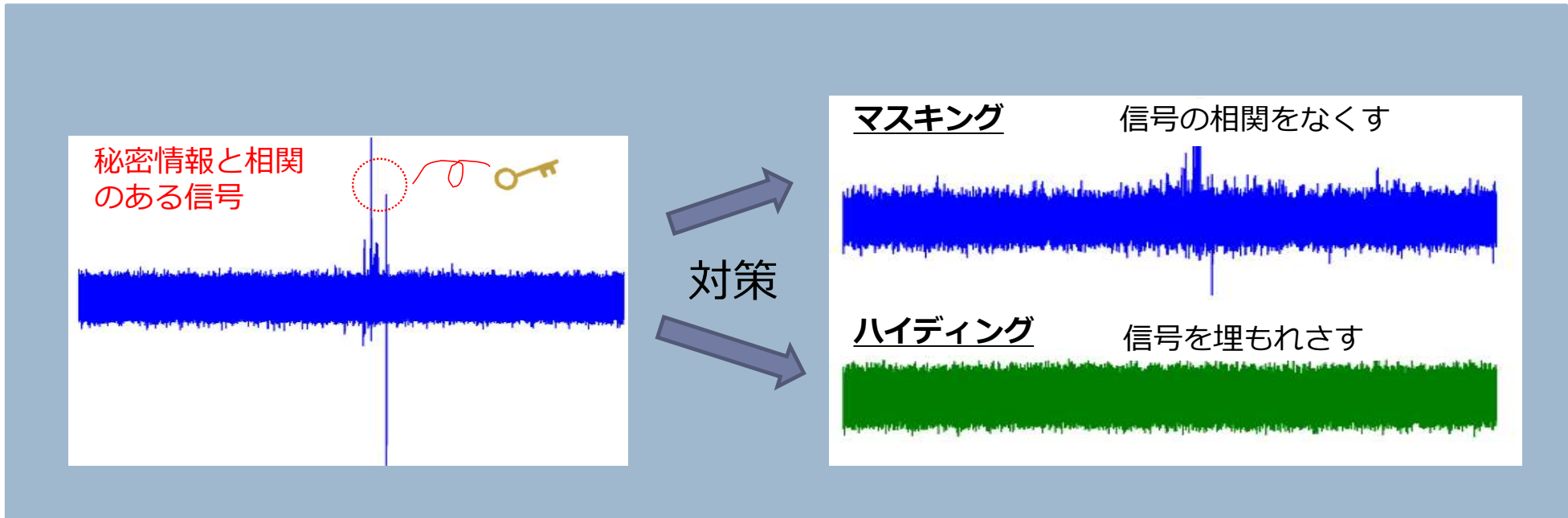
```
N =  b272bda6b2f8924c8fd64a6e8a53c109 6ee115e05c610b3da7fe4faeef2a0cf6
     3ec07ddd40901dec92a1d494533be2db e47c6c69979f6fa2d0f305da678a3a30
     58833047f73a42333935ccf7f138c3f3 2575b39ef0d84867f09316f582ae2c4e
     bf4e6c95963a4b9a96cab0b019e295b8 4aa6aace4a6d4df0c11972aaf1f2d223
     fc2a10a958206eebfb1460babd3113a5 90898e01cc7e6fccccfddb8429db7380
     207435d0412f90203d8193cc0dfe769c a7ae672c8aca164eebc46b1e32d51e9e
     f6e3c3b49ea749a6941de283c992a0ad cb1f1d8cbe7f00842246b8731353ec02
     44bc2df0a60e9b868ab48bd8cd0634e9 9abd5708a3a1e745c12e57fdd1c8a5d1 (256 byte)
```

この公開鍵**N**は，インクリメント数列が素数候補であるならば，素因数分解できるはずなので試してみたところ，次の2つの数**P，Q**が得られた．

```
P =  C8A37C7B26B647DBB2FF030688F3BCBE 9205FC89AAC845C88762A02D24E16AE2
     BBFD2BE3329E7954167F242E716F4A1C 3C494053C290360E346B591306C974B6
     CCA65C7B4064041A5262B2652B3D5453 D98C2C3102B4A85E3331F8FA2CBE1792
     E358E65000C14532FA487538E72DF537 2DC64825341D29BF03B15055FD6B8989 (128 byte)

Q =  E3AFCA404F926382043CF19B5F60EE67 401C3DF279A13E7EAF3E609874D37992
     CB38B0EDFE29EE0ED4E381AD975B5890 472F48F1C3C5EDB98CD7E4AE0195EEEA
     E01800E28D487CA24CF103239C7EF6A5 B3771AADC7F9E0CFEB06F48CC1DA4E44
     7A78C4A11506B765DD0C658132EFFA01 A38AA05F5CBFA188A7A2B820CA565009 (128 byte)
```

この **P，Q** について，**N-P*Q** を計算して **0** になることと，
P，Q を決定性アルゴリズム（APRCL）により素数判定して確かに素数であることの，２点を確認した．

サイドチャネル攻撃　　　サイドチャネル攻撃対策

D)フォールト攻撃研究事例

フォールト攻撃の概要

- 暗号モジュールに何らかの方法で誤動作（フォールト）を誘発し，計算誤りを引き起こすことで秘密情報を奪取するフォールト攻撃の脅威が指摘されている．
- 学術的には1997年にBonehらによって指摘された．

  [0] D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking crypto-graphic protocols for fault," EUROCRYPT 1997, LNCS, vol. 1233, pp.37-51, Springer, 1997.

- その後BihamらによってDESなどの共通鍵暗号に対しても誤りを含む暗号文と正規の暗号文のペアを複数取得し，それを解析するDFA (Differential Fault Analysis) という手法により鍵を導出できる可能性が指摘された．

  [1] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," CRYPTO 1997, LNCS, vol. 1294, pp.513-525, Springer, Aug. 1997.

- フォールトを起こす方法としては，クロックグリッチ，電源グリッチ，電磁波照射，レーザー照射等が挙げられる．

レーザー照射によるフォールト攻撃研究

- レーザーは照射位置精度と照射タイミングが正確なので再現性が高く、フォールト攻撃において強力な攻撃として研究が行われている。
- Skorobogatov らは文献[#1]において、SRAMの任意の1ビットを反転できることを、指摘している。
- Derouet は文献[#2]で、CPU回路のどの部分にレーザーを照射すると、どのようなフォールトが起こるかなどを詳細に報告している。
- 横浜国大では、レーザー照射を用いたソフトウェアに対する精密なフォールト注入により、プロセッサにおいて実行される機械語命令の任意の1bitを操作して別の命令に書き換える命令改変攻撃という強力な攻撃手法を報告している。さらに、ARMマイコン搭載の攻撃評価用カードであるTVCにおいて、命令の読み出し位置が2箇所に分かれていることを利用したレーザーフォールト攻撃対策が考えらえるが、これもダブルスポットレーザー照射装置を用いた2点への照射により無効化できることを示している[#3]。

[#1] S. Skorobogatov and R. Anderson, “Optical Fault Induction Attacks,” CHES 2002, LNCS 2523, pp. 2-12, 2003.
[#2] O. Derouet, “Secure Smartcard Designagainst Laser Fault Injection,”FDTC 2007, 2007.
[#3] 鈴木 朋郎, 坂本 純一, 松本 勉, “ダブルレーザー照射装置を用いたTVCに対する命令置換フォールト攻撃,” 信学技報, vol. 119, no. 143, HWS2019-33, pp. 221-225, 2019年7月.

フォールト攻撃の実際

クロックグリッチ
グリッチ
(ナノ~ピコ秒精度)
正常なクロック周期
(数M~1GHz)
クロック信号
電磁波照射
数百~数千V
の強力な
電磁パルス
レーザー照射
赤色 or
近赤外波長
数mW~数十W
攻撃者は様々な方法でデバイス
にフォールト（故障）を注入
フォールトによる影響をモデル化
＝フォールトモデル
ビットセットモデル
...0010... ➡ ...1110...
攻撃対象
(スマートフォン，クレジットカ
ード，スマートメータ，etc...)
命令スキップモデル
元の命令列
行
ニーモニック
1 add r1,1
2 mov r2,r0
3 sub r3,r3
命令スキップの例
行
ニーモニック
1 add r1,1
2 mov r2,r0
3 sub r3,r3
命令スキップモデル＝
最も一般的なモデル
命令スキップに対する対策
が多数提案されている
これらの対策を講じれば
本当にセキュアとなるか？

フォールト攻撃の進化形

デバイスへのレーザー照射によって

実行中の命令を別の命令へ改変できることがある

モデル化

命令改変モデル

元の命令列

行	ニーモニック
1	add r1,1
2	mov r2,r0
3	sub r3,r3

ある程度
任意の命令
に改変

何もしない命令への改変＝命令スキップだとみなせるため，
命令改変は命令スキップよりも強力

命令改変の例1

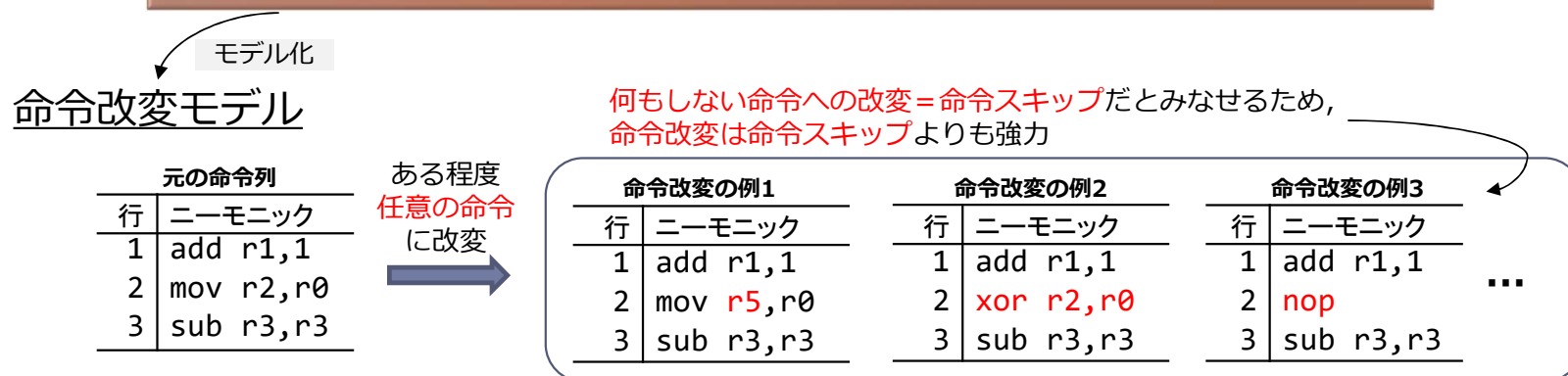
行	ニーモニック
1	add r1,1
2	mov r5,r0
3	sub r3,r3

命令改変の例2

行	ニーモニック
1	add r1,1
2	xor r2,r0
3	sub r3,r3

命令改変の例3

行	ニーモニック
1	add r1,1
2	nop
3	sub r3,r3

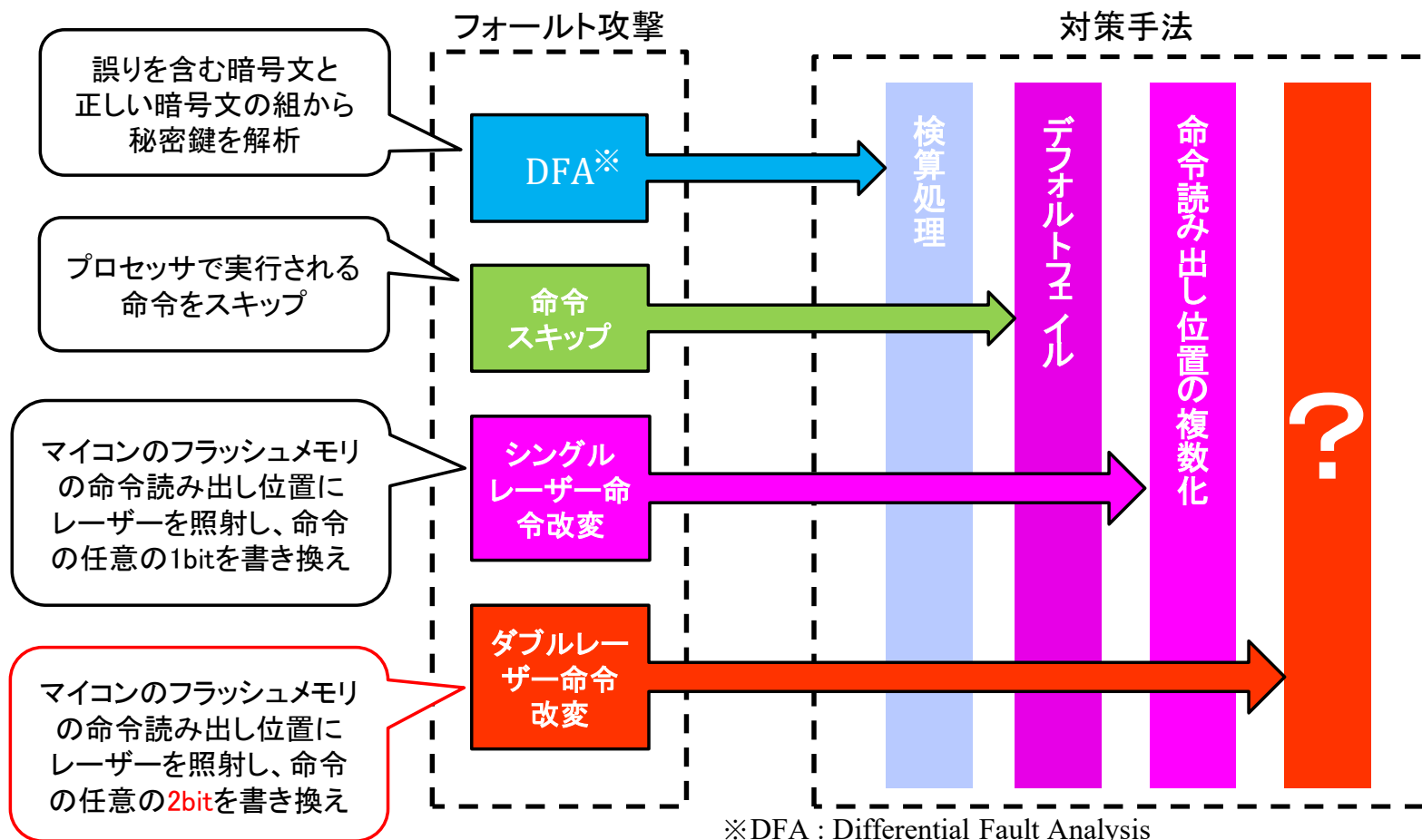
…

命令改変によって

- セキュアだと信じられてきた対策技術が攻撃できることがある
- 高機能暗号のような複雑な暗号システムも攻撃できることがある
  （高機能の例：暗号化したまま検索可能など）

- レーザー装置の高度化によるより強力な命令改変の可能性がある
- 命令改変対策が必要である

●暗号モジュールはフォールト攻撃への耐性が求められる。

- 暗号モジュールがどのような脆弱性をもつか、また実装されたフォールト攻撃対策が期待どおりの効果を発揮しているか、などを評価できることが望ましい。

※DFA : Differential Fault Analysis

フォールト攻撃に用いる故障解析技術の展開

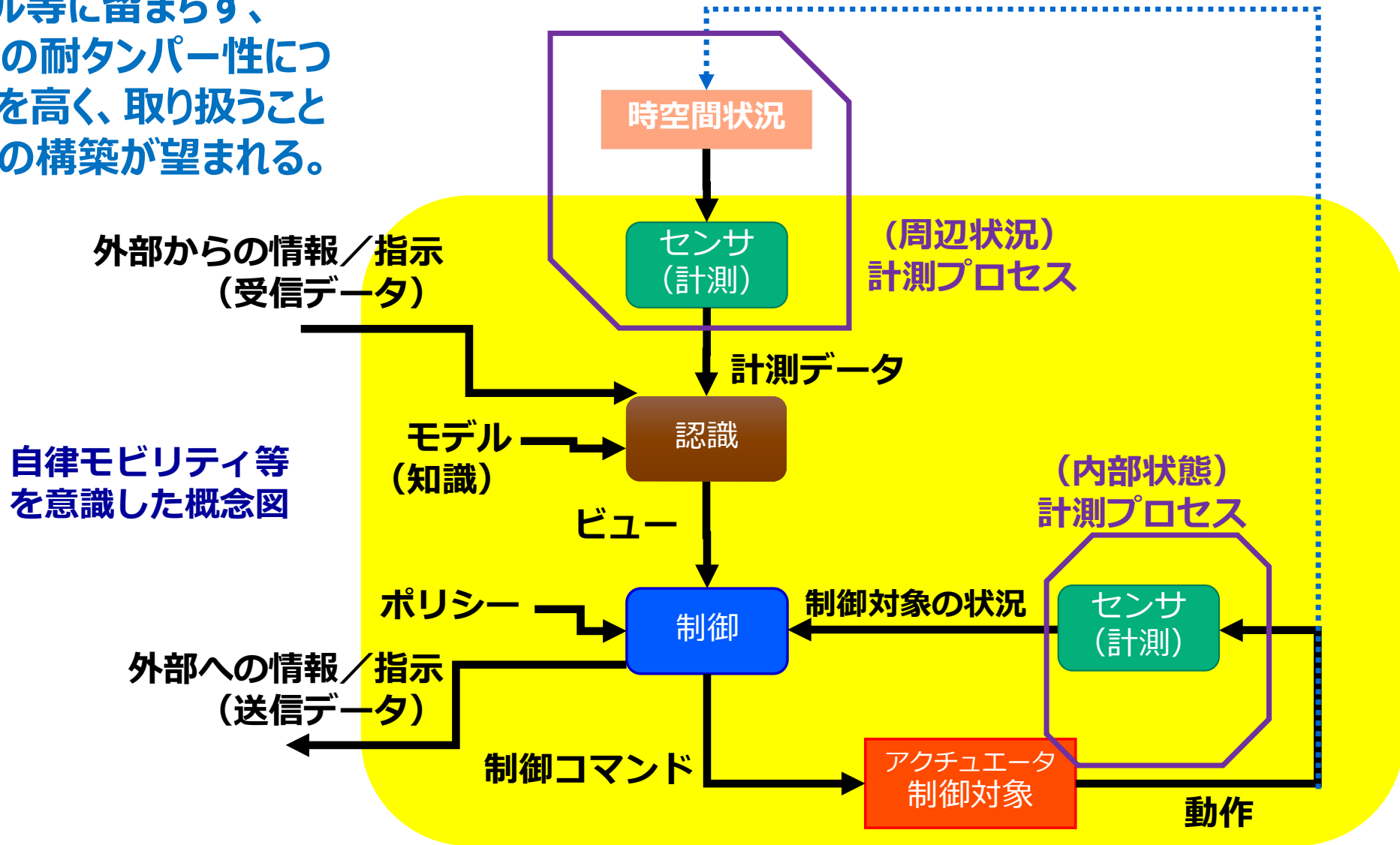
- 誤り暗号文が必要な手法と不要な手法に分けられる
- 前者に対しては暗号文の検算による対策が一般的

方式	概要	誤り暗号文
DFA [1]	誤り暗号文と正しい暗号文の差分から鍵を解析	必要
FSA [2]	最少の故障強度と中間値の相関関係をプロファイリングして鍵を推定	不要
IFA [3]	フォールト注入により暗号文が誤るか否かから鍵を推定	不要
SFA [4]	誤り暗号文を統計的に解析して鍵を推測	必要
SIFA [5]	誤らなかった暗号文(**Ineffective**暗号文)を統計的に解析	不要

[1] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In Annual international cryptology conference, pages 513–525. Springer, 1997.
[2] Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta. “Fault sensitivity analysis,” CHES, 2010.
[3] Christophe Clavier, “Secret external encodings do not prevent transient fault analysis,” IACR CHES, 2007.
[4] Fuhr, Thomas, et al. "Fault attacks on AES with faulty ciphertexts only,” FDTC, 2013.
[5] Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Stefan Mangard, Florian Mendel, and Robert Primas, “SIFA: exploiting ineffective fault inductions on symmetric cryptography,”, CHES, 2018.

E) 研究成果のアウトカム

- 上記事例のような実装攻撃等に関する研究結果は、既に組込み機器に使用されているICチップにおいて、その用途に対して期待されるサイドチャネル攻撃耐性やフォールト攻撃耐性を有するか否かを判定する際に役立つ。
- 暗号モジュール試験認証制度や、コモンクライテリア（情報システムセキュリティ評価認証精度）や、各種認証スキームにおけるサイドチャネルセキュリティの基準作成や製品の試験・評価にダイレクトに役立つ。
- これらの基準を参照して組込み機器のセキュリティ仕様を定めることにより、セキュアな機器の普及を促進する。

暗号モジュール等に留まらず、
機器そのものの耐タンパー性につ
いて、分解能を高く、取り扱うこと
のできる体系の構築が望まれる。
時空間状況
センサ
（計測）
（周辺状況）
計測プロセス
外部からの情報／指示
（受信データ）
計測データ
認識
モデル
（知識）
自律モビリティ等
を意識した概念図
ビュー
（内部状態）
計測プロセス
ポリシー
制御
制御対象の状況
センサ
（計測）
外部への情報／指示
（送信データ）
制御コマンド
アクチュエータ
制御対象
動作

- 暗号モジュール等に留まらず、機器そのものの耐タンパー性について、分解能を高く、取り扱うことのできる体系の構築が望まれる。

- 必要とされる耐タンパー性を経済的に達成するための技術革新に期待が高まっている。

- 例えば、経済安全保障重要技術育成プログラム（K Program）において本年7月から開始した「先進的サイバー防御機能・分析能力強化」においても「耐タンパー性向上技術」というテーマが設定され、
  耐タンパー技術の体系化と先端的技術の開発が進められている。

サイバーフィジカルセキュリティを支える先端技術と課題　～むすび～

- サイバーフィジカルシステムおよびその構成機器は各種サイバーフィジカル攻撃に対する適切なセキュリティを具備すべき。
- セキュリティは広範な分野であり、多様な課題がある。
- 多様な研究開発が世界規模で盛んに行われている。
- この講演では、既に我が国に強みのある高機能暗号技術は省略し、これから強みなることが期待される分野から耐タンパー技術を紹介した。
- 国立研究開発法人産業技術総合研究所ではサイバーフィジカルセキュリティ分野においても力を入れて優秀な人材と技術の研究開発と知識の蓄積活用に取り組んでいる。